১৪৩৩

তথ্য সুরক্ষায় একজন মুজাহিদের পাথেয়

ইনশাআল্লাহ

বইটির লক্ষ্য হচ্ছে জাহান্নামের কীট, কুফফারদের থেকে মুজাহিদ ভাইদের বিট ও বাইট কিছুটা সুরক্ষিত রাখা।

আনসারুল্লাহ আইটি টিম।

যারা আমাদের নাজাতের জন্য দু‘আ করবেন তাদের জন্য এই বইটি একদম ফ্রী।

১৭ রমজান ১৪৩৩ হিজরী
০৫ অগাষ্ট ২০১২ ঈসায়ী

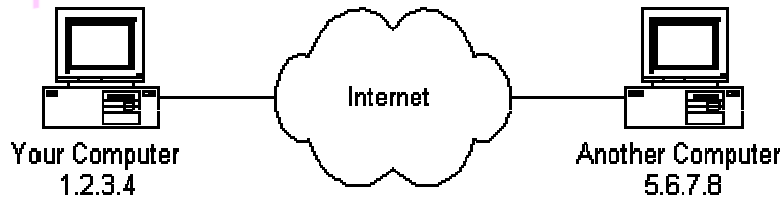
সূচীপত্র

১. ইন্টারনেট কিভাবে কাজ করে

(এই অধ্যায়টি ঐচ্ছিক, সবার জন্য জরুরী নয়)

১.১. আইপি এড্রেস

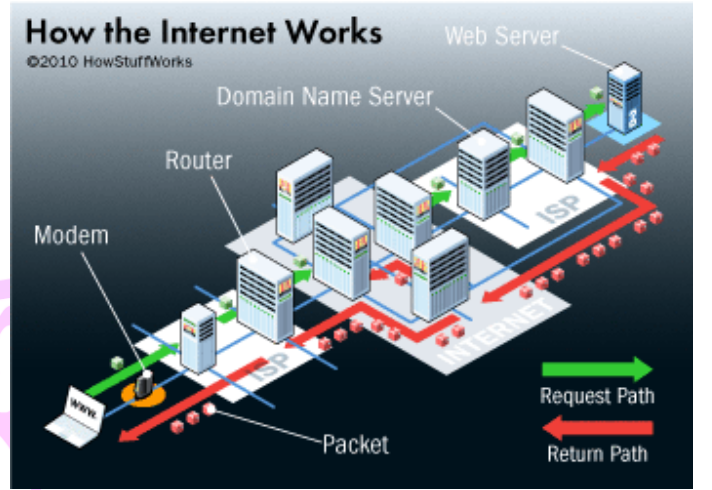
ইন্টারনেট হচ্ছে সারা পৃথিবীব্যাপী কম্পিউটারের এক বিশাল নেটওয়ার্ক। খুব স্বাভাবিকভাবেই ইন্টারনেটে সংযুক্ত (Connected) প্রতিটি কম্পিউটারের একটি স্বতন্ত্র এড্রেস থাকবে। ইন্টারনেট এড্রেস সাধারনত এই রকমের হয়ঃ nnn.nnn.nnn.nnn যেখানে nnn হচ্ছে ০০০-২৫৫ পর্যন্ত যেকোন সংখ্যা। এই এড্রেসকে আইপি এড্রেস (IP address) বলা হয়। IP মানে হলো ইন্টারনেট প্রোটোকল(Internet Protocol)। এ ব্যপারে আলোচনা সামনে আসছে ইনশাআল্লাহ।

নিচের ছবিতে ব্যাখ্যা করা হচ্ছে কিভাবে একটি কম্পিউটার (যার IP address 1.2.3.4) ইন্টারনেটের মাধ্যমে অপর একটি কম্পিউটার (যার IP address 5.6.7.8) এর সাথে সংযুক্ত হয়। এখানে ইন্টারনেট বলতে এই দুই কম্পিউটারের মধ্যে সংযোগ স্থাপনকারী একটা ব্যবস্থা বুঝানো হচ্ছে। পরে তা বিষদভাবে ব্যাখ্যা করা হবে।

চিত্র ১

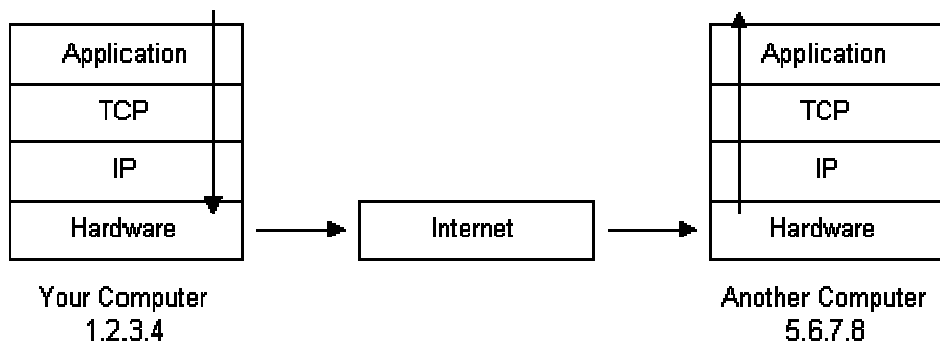
যদি আপনি কোন ইন্টারনেট সেবা দানকারী কোন প্রতিষ্ঠান (Internet Service Provider বা সংক্ষেপে ISP) এর সাথে সংযুক্ত হন (তা যে কোন ভাবেই হোক না কেন, যেমন ধরুন মডেম, ডায়াল-ইন, ওয়াই ফাই ইত্যাদি), তারা আপনার জন্য একটি স্বল্পমেয়াদী বা স্থায়ী IP address বরাদ্দ করে দিবে। সুতরাং বলা যায়, আপনি যখনি ইন্টারনেট ব্যবস্থার সাথে সংযুক্ত হবেন, তখনই আপনার কম্পিউটারের একটি স্বতন্ত্র IP address থাকবে।

১.২. প্রোটোকল সারি ও প্যাকেট

ধরে নিন আপনার কম্পিউটার এখন ইন্টারনেটের সাথে সংযুক্ত এবং আপনার স্বতন্ত্র IP address 1.2.3.4, এখন প্রশ্ন হলো আপনার কম্পিউটার কিভাবে ইন্টারনেটে সংযুক্ত অপর কম্পিউটারের (যার স্বতন্ত্র IP address 5.6.7.8) সাথে কিভাবে কথা বলবে (যোগাযোগ করবে)? উদাহরণস্বরুপ আপনি একটা মেসেজ দিতে চান "হ্যালো কম্পিউটার 5.6.7.8"। ধরুন আপনি আপনার বাসায় বসে ডায়ালিং এর মাধ্যমে আপনার ISP এর সহায়তায় ইন্টারনেটে সংযুক্ত হয়েছেন। তাহলে আপনার লিখা মেসেজটা অবশ্যই কেবলের (ফোন লাইন) মাধ্যমে ইন্টারনেটে স্থানান্তরিত হতে হবে। তাই আপনার লিখা মেসেজটাকে অবশ্যই ইলেকট্রনিক সিগনালে পরিবর্তন করতে হবে, আর এই ইলেকট্রনিক সিগনালটা ইন্টারনেটের মাধ্যমে সঞ্চালিত হবে এবং অবশেষে এই ইলেকট্রনিক সিগনালটা পুনরায় শাব্দিক মেসেজে পরিবির্তিত করতে হবে।

কিভাবে এই কাজটা করা সম্ভব? প্রোটোকলসারি ব্যবহার করার মাধ্যমে এই কাজটা করা সম্ভব। ইন্টারনেটের মাধ্যমে যোগাযোগ প্রতিষ্ঠার জন্য প্রতিটি কম্পিউটারের এ ধরণের একটি প্রোটোকলসারির প্রয়োজন। সাধারণত কম্পিউটারের অপারেটিং সিস্টেমেই তা তৈরী করা থাকে। ইন্টারনেট ব্যবহারের জন্য যে প্রোটোকলসারির দরকার হয় তাকে TCP/IP protocol stack বা TCP/IP প্রোটোকলসারি (কারণ এখানে দুটি বড় ধরণের যোগাযোগ প্রোটোকল ব্যবহার করা হয়ঃ TCP এবং IP) বলা হয়।

TCP/IP প্রোটোকলসারি দেখতে অনেকটা এরকমঃ

প্রোটোকল স্তর	মন্তব্য
এপ্লিকেশান প্রোটোকল স্তর	প্রোটোকল যা নির্দিষ্ট এপ্লিকেশান এর জন্য রাখা হয়ঃ যেমনঃ WWW (world wide web), e-mail, FTP (File Transfer Protocol যা file আপলোড বা ডাউনলোড করতে প্রয়োজন হয়) ইত্যাদি।
ট্রান্সমিশান কন্ট্রল প্রোটোকল (TCP) স্তর	TCP একটা port number (যা পরে ব্যখ্যা করা হবে) ব্যবহার করে কোন তথ্য প্যাকেটকে একটা কম্পিউটারের নির্দিষ্ট এপ্লিকেশানে পাঠায়।
ইন্টারনেট প্রোটোকল (IP) স্তর	IP ওই তথ্য প্যাকেটকে IP address এর সহায়তায় একটি নির্দিষ্ট কম্পিউটারে প্রেরণ করে।
হার্ডওয়্যার স্তর	বাইনারী প্যাকেটকে নেটওয়ার্ক সিগনাল এ রূপান্তর করে (এবং বিপরীত রূপান্তরও করে) যেমনঃ মডেম।

আমরা যদি “হ্যালো কম্পিউটার 5.6.7.8” মেসেজটার গমন পথ অনুসরণ করি, যা আমাদের কম্পিউটার থেকে অপর কম্পিউটারে (যার IP address 5.6.7.8) যাচ্ছে, তাহলে আমরা দেখতে পাবোঃ

চিত্র ২

১। মেসেজটা TCP/IP প্রোটোকলসারির উপর থেকে চলা শুরু করবে এবং নিচের দিকে নামতে থাকবে।

২। যদি মেসেজটা খুব বড় হয়, তবে প্রতিটি প্রোটোকলসারি মেসেজটিকে ছোট ছোট ভাগে ভাগ করবে, এই ছোট ছোট তথ্যের কণাকে আমরা তথ্য প্যাকেট বলি।

৩। প্যাকেটটি এপ্লিকেশান প্রোটোকল স্তর অতিক্রম করে TCP স্তরে যায় যেখানে প্রতিটি প্যাকেটের জন্য একটি port number বরাদ্দ করা থাকে।

৪। অতপর প্যাকেটটি IP স্তর এ যায়। এইখানে প্রতিটি প্যাকেট তার গন্তব্যস্থলের ঠিকানা 5.6.7.8. পেয়ে যায়।

৫। এখন আমাদের মেসেজ প্যাকেটটার একটা port number এবং একটা IP address আছে। এটা এখন ইন্টারনেটে প্রেরণের জন্য তৈরী। এখন হার্ডওয়্যার স্তর আমাদের প্যাকেটের ডাটাকে ইলেকট্রনিক নেটওয়ার্ক সিগনালে রুপান্তর করে এবং তা কেবলের মাধ্যমে স্থানান্তর করে।

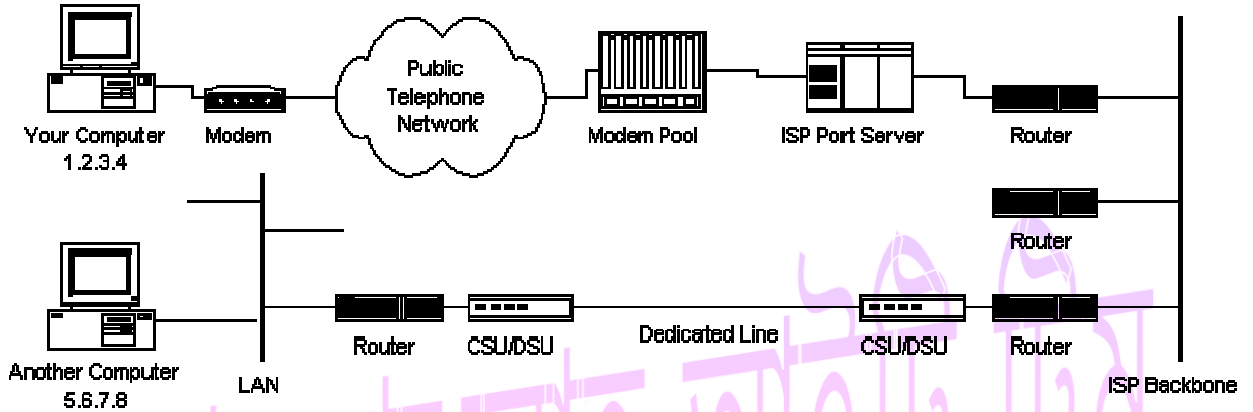
৬। কেবলের অপর প্রান্তে আপনার ISP সরাসরি ইন্টারনেটের সংযুক্ত। ISP এর router (রাউটার) প্রতিটি প্যাকেটের গন্তব্য ঠিকানা নিরীক্ষণ করে এবং কোথায় তাকে পাঠানো হবে তা নির্ধারণ করে। প্রায়শই এই প্যাকেটটাকে অপর আরেকটি router (রাউটার) এ পাঠানো হয়। router (রাউটার) সংক্রান্ত আলোচনা পরে করা হবে।

৭। পরিশেষে প্যাকেটটি তার গন্তব্য কম্পিউটারে (যার IP address 5.6.7.8) পৌছে। এখানে প্যাকেটটি TCP/IP প্রোটোকলসারির নিচ থেকে চলা শুরু করবে এবং উপরের দিকে উঠতে থাকে।

৮। যখন প্যাকেটটি TCP/IP প্রোটোকলসারির উপরের দিকে উঠতে থাকে, তখন প্রেরক কম্পিউটার প্যাকেটটির সাথে যেসব ডাটা সংযুক্ত করেছিল (যেমনঃ IP address and port number) তা প্যাকেটটি থেকে অপসারণ করা হয়।

৯। যখন প্যাকেটটি সারির একেবারে উপরে উঠে যায় তখন প্যাকেটগুলো পুনরায় একসাথে করা হয় এবং তার মুল অবস্থায় ফিরিয়ে নেয়া হয়। পাঠক তখন মেসেজটা পড়তে পারেঃ "হ্যালো কম্পিউটার 5.6.7.8"।

১.৩. নেটওয়ার্কের অবকাঠামো

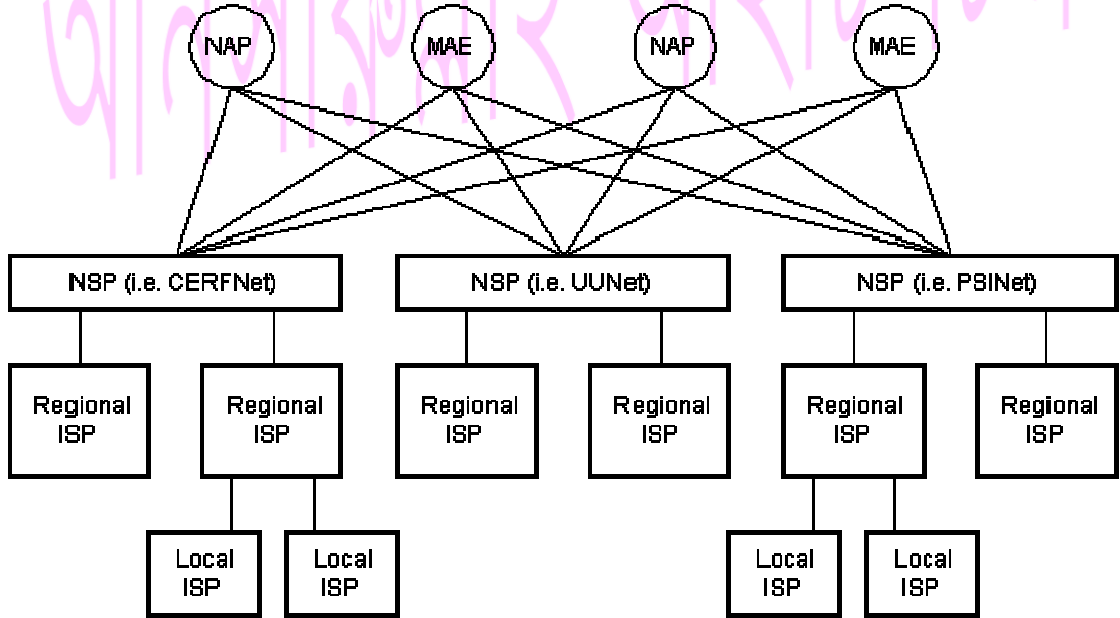
আমরা এখন জানি কিভাবে একটা প্যাকেট এক কম্পিউটার থেকে অন্য কম্পিউটারে ইন্টারনেটের মাধ্যমে গমণ করে। কিন্তু এর মধ্যবর্তী বিষয়গুলো আমরা এখনো জানি না। আমরা এখন জানবো কি কি উপাদান নিয়ে ইন্টারনেট সঠিত হয় এবং এই উপাদানগুলোর কাজ কি? নিচের চিত্রটা একটু মনোযোগ দিয়ে দেখিঃ

চিত্র ৩

এখানে আসলে চিত্র ১ কে আরও বিস্তারিত ভাবে চিত্রায়িত করা হয়েছে। আমাদের কম্পিউটার থেকে Internet Service Provider পর্যন্ত কিভাবে কানেকশান হচ্ছে তা আমাদের জন্য সহজবোধ্য হলেও এর পরবর্তী ধাপগুলো বিস্তারিতভাবে জানতে হবে।

ISP সাধারণত তাদের কাস্টমারদের জন্য একটি পুল (অনেক মডেমের স্বমন্বয়ে গঠিত) চালনা করে। এটা সাধারণত একটা কম্পিউটার দ্বারা করা হয় যা মডেম পুল থেকে ISP Backbone বা কোনো router এর মধ্যকার ডাটা প্রবাহ নিয়ন্ত্রণ করা যায়। এই ব্যবস্থাকে অনেক সময় port server ও বলা হয়।

যখন আপনার প্যাকেটটি আপনার ফোন নেটওয়ার্ক থেকে আপনার ISP এর সরঞ্জামে এসে পৌছলো তখন আপনার প্যাকেটটি ISP এর Backbone গমণ করে। সেখান থেকে প্যাকেটটি আরও অনেক router ও Backbone দিয়ে যায়, যে পর্যন্ত না তা তার সঠিক গন্তব্যে (যার IP address 5.6.7.8) না পৌছে। এখানে বলে রাখা ভালো Internet routers হচ্ছে একটি ব্যবস্থা যা নির্ধারণ করে আপনার প্যাকেটটিকে কোথায় পাঠানো হবে।

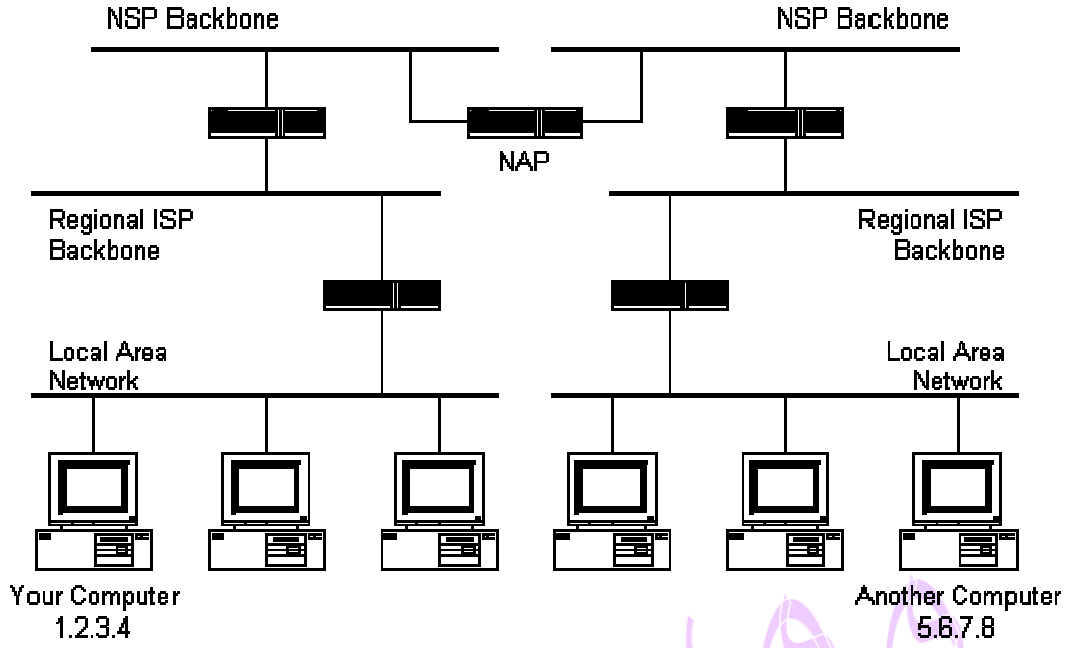
১.৪. ইন্টারনেট অবকাঠামো

ইন্টারনেট backbone হচ্ছে অনেকগুলো বড় বড় নেটওয়ার্কের সমন্বয়ে গঠিত একটা ব্যবস্থা যেখানে প্রতিটি নেটওয়ার্ক একে অপরের সাথে সম্পর্কযুক্ত। এইসব বড় বড় নেটওয়ার্ক গুলোকে বলা হয় Network Service Providers (নেটওয়ার্ক সার্ভিস প্রোভাইডার) বা NSPs। উল্লেখযোগ্য কিছু NSPs হচ্ছেঃ UUNet, CerfNet, IBM, BBN Planet, SprintNet, PSINet। এই নেটওয়ার্কগুলো একে অপরের সাথে সমন্বয় সাধন করে যেন তারা নিজেদের মধ্যে প্যাকেট আদান-প্রদান করতে পারে। প্রতিটি NSP তিনটি Network Access Points or NAPs এর সাথে সংযুক্ত। এই NAPs এ, কোনো প্যাকেট একটি NSP এর backbone থেকে অপর NSP backboneএ জাম্প করতে পারে। এই NSP গুলো আবার Metropolitan Area Exchanges or MAEs তে ও ইন্টার-কানেক্টেড (নিজেদের মধ্যে কানেক্টেড)। MAEs এর কাজ আর NAPs এর কাজ একই, কিন্তু MAEs গুলো ব্যক্তি মালিকানাধীন। এদের উভয়কেই (NAPs এবং MAEs) Internet Exchange Points (ইন্টারনেট বিনিময় পয়েন্ট) or IXs বলা হয়। NSP গুলো সাধারণত ISP (Internet Service Provider) গুলোর কাছে bandwidth (ব্যান্ডউইডত) বিক্রি করে থাকে। নিচের চিত্রে এই অবকাঠামো বিভিন্ন স্তরে বিন্যস্থ করে দেখানো হয়েছেঃ

চিত্র ৪

উপরের চিত্র একটি সাধারণ ও সরল চিত্র যাতে দেখানো হয়েছে কিভাবে NSP গুলো নিজেদের সাথে ও বিভিন্ন ছোট ISP গুলোর সাথে সংযোগ স্থাপন করে। প্রকৃত চিত্র আরও জটিল আকৃতির।

১.৫. ইন্টারনেট রাউটিং বা গমণপথ স্তর

কিভাবে প্যাকেটগুলো ইন্টারনেটে তাদের নির্দিষ্ট পথ খুজে পায়? ইন্টারনেটে সংযুক্ত প্রতিটি কম্পিউটার কি জানে অন্য কম্পিউটারগুলো কোথায় রয়েছে? প্যাকেট গুলোকে কি সকল কম্পিউটারে প্রচার করা হয়? উপরের প্রশ্ন দুটির উত্তর হচ্ছে 'না'। কোনো কম্পিউটারই জানে না অন্য কম্পিউটারগুলো কোথায় রয়েছে আর প্যাকেটগুলোও সব কম্পিউটারে যায় না। প্যাকেটগুলোকে তাদের সঠিক গন্তব্যস্থলে পৌছানোর জন্য যে সকল তথ্যের দরকার তা routing tables এ দেয়া থাকে, আর এই routing tables গুলো প্রতিটি router ধারণ করে রাখে। এটাই হচ্ছে ইন্টারনেটে একটা router এর কাজ।

Routers হচ্ছে প্যাকেট অদল-বদল কারী। একটা router সাধারণত কিছু নেটওয়ার্কের মধ্যে সংযুক্ত থাকে যেন এই নেটওয়ার্কগুলোর মাঝে প্যাকেট যাবার একটা ব্যাবস্থা করে দিতে পারে। প্রতিটি router জানে তার অধীনস্থ নেটওয়ার্কে কারা আছে আর তারা কি IP address ব্যবহার করছে। কিন্তু একটা router সাধারণত জানে না তার উপরের IP address গুলো কি। নিচের চিত্রটি নিরীক্ষণ করুন। যে সব কালো বাক্স backbone গুলোকে সংযুক্ত করে রেখেছে তারা হচ্ছে router. উপরের দিকের বড় NSP backbone গুলো একটা NAP এ সংযুক্ত আছে। তাদের নিচে কিছু সাব-নেটওয়ার্ক আছে এবং তাদের নিচে আরও কিছু সাব-নেটওয়ার্ক আছে, একেবারে নিচের দিকে দুটি লোকাল এরিয়া নেটওয়ার্ক এ কম্পিউটারগুলো সংযুক্ত আছে।

চিত্র ৫

যখন কোনো প্যাকেট একটি router এ আসে, ওই router টা তখন প্রেরক কম্পিউটারের IP protocol layer যে IP address দিয়েছে তা পরীক্ষা করে দেখে। Router তখন তার routing table চেক করে। যদি ওই IP address সংশ্লিষ্ট নেটওয়ার্ক খুজে পাওয়া যায়, তবে প্যাকেটটা সেই নেটওয়ার্কে পাঠানো হয়। আর যদি না পাওয়া যায় তবে ওই router সেই প্যাকেটটা অন্য একটা default route এ পাঠিয়ে দেয় যা সাধারণত backbone স্তরে উপরের দিকে থাকে। আশা করা যায় যে পরবর্তী router জানে কোথায় packet টা পাঠাতে হবে। যদি সে তা না জানে, তাহলে ওই packet টা আগের মতই উপরের দিকে উঠতে থাকে যতক্ষণ না সে একটি NSP backbone গিয়ে না পৌছে। যেসব router, NSP backbone গুলোতে সংযুক্ত রয়েছে তাদের routing table হচ্ছে সবচেয়ে বড় এবং ওই packet টা কে সঠিক backbone এ তখন পাঠানো হয়, সেখান থেকে তা (প্যাকেটটা) নিচের দিকে যেতে থাকে ক্ষুদ্র ক্ষুদ্র নেটওয়ার্কের মধ্য দিয়ে যতক্ষণ না সে তার গন্তব্যস্থলে পৌছে।

১.৬. ডোমেইন নাম ও ঠিকানা

যদি আপনি সেই কম্পিউটার এর IP address না জানেন যার সাথে আপনি যুক্ত হতে চান, তখন কি হবে? যদি আপনার web server এর মাধ্যমে আপনাকে *www.anothercomputer.com* নামক কোনো ঠিকানায় যেতে হয়, তখন আপনি কি করবেন? আপনার web browser কিভাবে জানবে এই কম্পিউটার ইন্টারনেটের কোথায় অবস্থান করছে? এই প্রশ্নের উত্তর হচ্ছে Domain Name Service or DNS. DNS হচ্ছে একটা বিস্তৃত তথ্য ভান্ডার (distributed database) যেখানে ইন্টারনেটে সংযুক্ত সকল কম্পিউটারের নাম ও তাদের IP address এর তালিকা রাখা হয়।

অনেক কম্পিউটার রয়েছে যা Internet host এ সংযুক্ত (connected), এরা এই DNS database এর একটা অংশ যা অন্য কম্পিউটারদের এই database এ প্রবেশ করার সুযোগ দেয়। এই সব বিশেষ কম্পিউটারদেরকে DNS servers বলা হয়। কোনো DNS server ই সম্পূর্ণ database ধারণ করে না, বরং এর একটা অংশ ধারণ করে। মনে করুন কোনো একটি কম্পিউটার একটা domain name (যেমনঃ *www.anothercomputer.com*) request করলো যা এই DNS server ধারণ করে না, তবে ওই DNS server সেই request কে অন্য DNS server এর দিকে ধাবিত (re-direct) করে দিবে। যখন আপনার request করা domain name এর সাথে সঙ্গতিপূর্ণ IP address খুঁজে পাওয়া যায় তবে browser তখন আপনাকে সেই গন্তব্য computer এর সাথে সংযুক্ত করে দিবে এবং আপনি যে web page দেখতে চাচ্ছেন তার জন্য সুপারিশ করবে।

১.৭. এপ্লিকেশান প্রটোকল

প্রটোকল সারিতে ইতোমধ্যে এ ব্যাপারে ইঙ্গিত দেয়া হয়েছে, কেউ হয়ত ধারণা করতে পারছেন যে ইন্টারনেট ব্যবহারের জন্য অনেক ধরণের Protocol ব্যবহার করতে হয়। এটা সত্য যে, ইন্টারনেট সঠিকভাবে কাজ করার জন্য অনেক ধরণের যোগাযোগ (communication) protocol দরকার। এদের মধ্যে উল্লেখযোগ্য হচ্ছেঃ TCP এবং IP protocols, routing protocols, medium access control protocols, application level protocols ইত্যাদি। নিচের অনুচ্ছেদে কিছু গুরুত্বপূর্ণ ও কমন protocols নিয়ে আলোচনা করা হলো Higher level protocols নিয়ে প্রথমে আলোচনা করা হবে, পরে lower level protocols নিয়ে আলোচনা করা হবে।

World Wide Web (WWW) হচ্ছে ইন্টারনেটে সবচেয়ে বেশী ব্যবহৃত সার্ভিস। যে application protocol এর জন্য web কাজ করতে সক্ষম হয় তা হচ্ছে Hypertext Transfer Protocol or HTTP. আপনারা আবার এর সাথে Hypertext Markup Language (HTML) কে গুলিয়ে ফেলবেন না। HTML হচ্ছে এক ধরণের ল্যাংগুয়েজ যা ব্যবহার করা হয় ওয়েব পেইজ লেখার জন্য। HTTP হচ্ছে এক ধরণের protocol যার মাধ্যমে ইন্টারনেটে ওয়েব ব্রাউজার (web browsers) এবং ওয়েব সার্ভার (web servers) একে অপরের সাথে যোগাযোগ করেন। এটা হচ্ছে একটি এপ্লিকেশান স্তরের প্রোটোকল কারণ প্রটোকল সারিতে তা TCP স্তর বা layer এর উপরে থাকে।

১.৭.১. HTTP এবং WWW (World Wide Web)

HTTP হচ্ছে একটি সংযোগবিহীন text based protocol. এখানে গ্রাহক বা Clients (web browsers) ওয়েব সার্ভার (web servers) কে request পাঠায় কোন ওয়েব উপাদান (web elements) যেমনঃ ওয়েব পেইজ বা ইমেজের জন্য। request টা সার্ভার কর্তৃক প্রদান করার পর গ্রাহক বা Client এবং ওয়েব সার্ভার (web servers) এর মধ্যে সংযোগ বিচ্ছিন্ন হয়ে যায়। প্রতিটি নতুন request এর জন্য বারবার নতুন সংযোগ স্থাপন করতে হয়। অধিকাংশ protocols হচ্ছে সংযোগ সংশ্লিষ্ট (connection oriented). এর মানে হচ্ছে যে দুটি কম্পিউটার যারা একে অপরের সাথে যোগাযোগ করছে, তাদের সবসময়ের জন্যই ইন্টারনেট এ সংযোগ চালু রাখতে হয়। HTTP হচ্ছে এর ব্যতিক্রম। client যখনই কোন . একটি HTTP request করতে চাইবে, সার্ভার এর সাথে এজন্য অবশ্যই নতুন কানেকশান বা সংযোগ স্থাপন করতে হবে। যখনই আপনি আপনার web browser এ একটি URL টাইপ করেন, তখনই নিচের ঘটনা ঘটতে থাকেঃ

১। যদি URL এ একটা domain name (যেমনঃ www.anothercomputer.com) থাকে, তাহলে browser প্রথমে একটি domain name server (DNS) এ সংযোগ স্থাপন করবে এবং ওই web server এর জন্য বরাদ্দকৃত IP address খুঁজে নিবে।

২। web browser তখন web server এর সাথে সংযোগ (connect) স্থাপন করবে এবং একটা HTTP request পাঠাবে (protocol stack বা সারির সহায়তায়) তার কাঙ্ক্ষিত web page এর জন্য।

৩। যদি server সেই web page টা খুজে পায় তবে web server তা পাঠায় আর যদি খুঁজে না পায় তবে একটি HTTP 404 error message পাঠায়। (404 means 'Page Not Found' বা পেইজ খুঁজে পাওয়া যায়নি।)

৪। web browser তখন page টা receive করে এবং connection তখন বিচ্ছিন্ন হয়ে যায়।

১.৭.২. এস.এম.টি.পি (SMTP) এবং ইলেক্ট্রনিক মেইল (email)

আরেক ধরণের ইন্টারনেট সার্ভিস হচ্ছে electronic mail বা E-mail. E-mail একটি এপ্লিকেশান স্তরের প্রোটোকলব্যবহার করে যার নাম Simple Mail Transfer Protocol বা SMTP. SMTP ও একধরণের text based protocol কিন্তু তা HTTP এর মত নয়, কারণ SMTP হচ্ছে সংযোগ সংশ্লিষ্ট (connection oriented) protocol।

যখন আপনি আপনার mail client খুলে আপনার e-mail পড়েন, তখন নিচের ঘটনাগুলো ঘটতে থাকেঃ

১। mail client (যেমনঃ Netscape Mail, Lotus Notes, Microsoft Outlook ইত্যাদি) তাদের mail server এ সংযোগ স্থাপন করে। mail server এর IP address বা domain name সাধারণত সেট করা থাকে যখন আপনি mail client ইনস্টল করেন।

২। client কি তার মেইল চেক করছে বা মেইল সেন্ড করছে এর উপর নির্ভর করে যথোপযুক্ত SMTP commands বা নির্দেশ server এর কাছে পাঠানো হয় আর সেই commands এর প্রতিউত্তর ও হয় সে অনুযায়ী।

২. টর ব্রাউজার

২.১. টর পরিচিতি (Tor)

টর হচ্ছে ভার্চুয়াল সুড়ঙ্গের (tunnels) এমন এক ধরণের নেটওয়ার্ক যাতে যে কোন ব্যক্তি বা দল তাদের ইন্টারনেট ব্যবহারের ক্ষেত্রে নিজেদের গোপনীয়তা এবং নিরাপত্তা বজায় রাখতে পারে। টর প্রথমে আপনার পাঠানো যেকোন তথ্যকে টর নেটওয়ার্কের তিনটি বিচ্ছিন্ন সার্ভার (যা রিলে সার্ভার বা relays নামে পরিচিত) এর মধ্য দিয়ে পাঠায়, অতঃপর আপনার সিগন্যালটি পাবলিক ইন্টারনেট (যেমনঃ ইয়াহু) এ পাঠানো হয়।

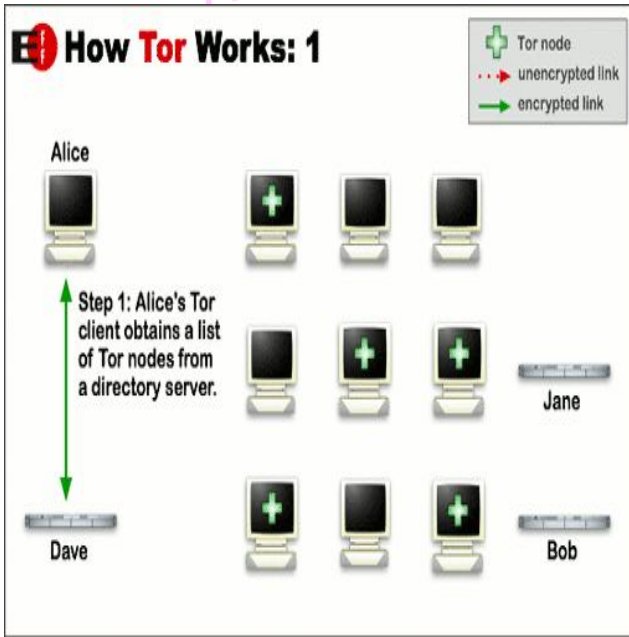
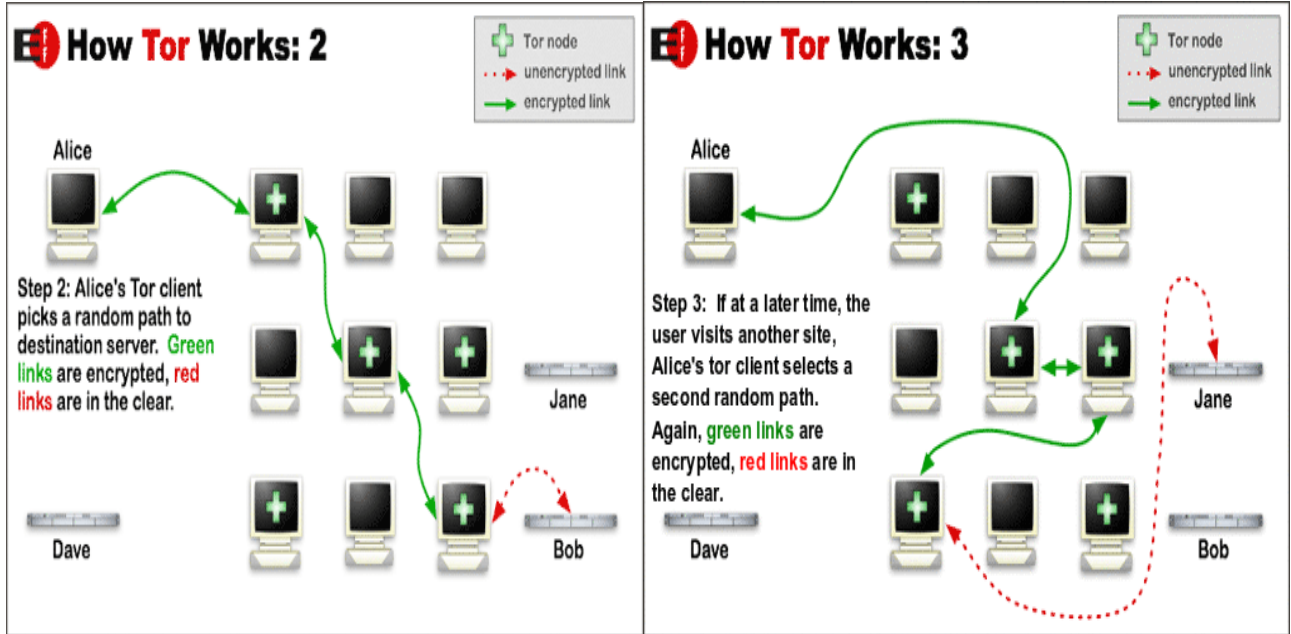
আপনি কোন কোন সাইট ভিজিট করেছেন আপনার ইন্টারনেট সংযোগ এর উপর নজরদারি করে কী বলতে পারবে। কিন্তু টর এই বিষয়টাকে প্রতিহত করতে পারে। আবার এমনও হতে পারে আপনি যেসব সাইট এ যাচ্ছেন সেইসব সাইট আপনার অবস্থান (আপনি কোথায় বসে ইন্টারনেট ব্যবহার করছেন) এর উপর নজর রাখছে। টর এসব সাইটকে আপনার উপর নজরদারী করা থেকে বিরত রাখে। এই ধরণের সেচ্ছাসেবক রিলে সার্ভার গুলোকে টর নেটওয়ার্ক বলা হয়।

কর্মদক্ষতার জন্য টর সফটওয়্যার সাধারণত কোন এক নির্দিষ্ট সময়ের জন্য (প্রায় দশ মিনিট বা তার কাছাকাছি সময়) একই সার্কিট বা পথ ব্যবহার করে। তাই এই সময়ের পরে আপনার নতুন request গুলো অন্য একটি সার্কিট বা পথ ব্যবহার করে। তাই আপনার কিছু সময় পূর্বের কাজের সাথে পরবর্তী কাজের কোন যোগসূত্র খুঁজে পাওয়া অন্য কোন লোকের পক্ষে সম্ভব নয়।

টর সব ধরণের গোপনীয়তা বজায় রাখতে পারে না। যেমনঃ এটা আপনার ডাটা প্রবাহের ব্যাপারে নিরাপত্তা দিতে পারে না। এখন যদি আপনি আপনার ডাটা (পরিচয় সংশ্লিষ্ট তথ্য বা Login ID and Password) সুরক্ষিত রাখতে চান সেক্ষেত্রে আপনাকে প্রটোকল সংশ্লিষ্ট সুনির্দিষ্ট সহায়ক সফটওয়্যার (protocol-specific support software) ব্যবহার করতে হবে। যেমনঃ আপনি ব্রাউজ করার ক্ষেত্রে টর বাটন (Torbutton) ব্যবহার করতে পারেন যা আপনার কম্পিউটারের কনফিগারেশান

(configuration) বিষয়ক কিছু তথ্য লুকিয়ে রাখতে সাহায্য করবে। বর্তমানে টর সফটওয়ারের সাথে আগে থেকেই কিছু টর বাটন যোগ করা থাকে।

২.২. টর ব্রাউজারের কর্মপদ্ধতি

টরের মাধ্যমে একটা গোপনীয় সংযোগ পথ (private network pathway) তৈরী করার জন্য, টর নেটওয়ার্কে ব্যবহারকারীর সফটওয়্যার বা client ক্রমাগতভাবে ও ব্যাপকভাবে relay ব্যবহারের মাধ্যমে একটি সাংকেতিক সংযোগ (encrypted connection) বিশিষ্ট পথ বা circuit তৈরী করে। এই পথ বা circuit একসাথে একই সময়ে কেবলমাত্র একটিই hop পর্যন্ত বিস্তৃত থাকে এবং প্রতিটি relay কেবলমাত্র শুধু এটুকু জানে যে, কোন relay তাকে এই ডাটা দিয়েছে এবং কোন relay কে সে ডাটা দিচ্ছে। একটি relay কখনোই জানে না যে ডাটা প্যাকেটটার সম্পূর্ণ পথটা কি। পুরো পথ বা circuit এ চলার সময় client প্রতিটি hop এর জন্য এক সেট আলাদা সাংকেতিক কোড ব্যবহার করে এটা নিশ্চিত করার জন্য যে প্রতিটি hop যেন এটা বুঝতে না পারে যে তারা কোন সংযোগ অতিক্রম করে এসেছে।

টর কেবলমাত্র TCP streams (transmission control protocol) এর জন্য কাজ করে এবং তা যে কোন এপ্লিকেশান দ্বারা ব্যবহার করা যাবে যদি ঐসব এপ্লিকেশান SOCKS support করে। এ কারণে যে সব প্রোগ্রাম TCP/IP প্রটোকল ব্যবহার করে না, সেগুলি টর এর ভিতর দিয়ে চালানো যাবে না।

টর যে তিনটি সার্ভার ব্যবহার করে তার মধ্যে দুটি সার্ভার আপনার পাঠানো সিগন্যালকে এনপক্রিপ্টেড (encrypted- বিভিন্ন সাংকেতিক চিহ্ন বা code দ্বারা রক্ষিত) করতে পারে। কিন্তু অবশিষ্ট সার্ভার (যা exit node নামে পরিচিত) তা করতে পারে না। এর মানে হলো এমন অনেক টর ব্যবহারকারী পাওয়া যাবে যাদের e-mail passwords খুব সহজেই বের করা যাবে (যদি তারা https ছাড়া ব্যবহার করে)। যেহেতু আমাদের আইডি হবে একটা মিথ্যা (বা fake) আইডি, তাই এই বিষয়টা খুব বড় কোনো ইস্যু নয়। তাছাড়া আমরা সব সময় https প্রোটোকল ব্যবহার করার চেষ্টা করবো।

টর এর গোপনীয়তা তার ব্যবহারকারীদের সংখ্যার উপর নির্ভর করে। টর নেটওয়ার্কের মধ্যে আপনাকে অন্যান্য ব্যবহারকারীদের মাঝে আড়াল করে রাখে। তাই যত বেশী মানুষ টর ব্যবহার করবে, টর তত বেশী নিরাপদ হবে অর্থাৎ আপনি তত বেশী গোপনীয়তা অবলম্বন করতে পারবেন। টরের ব্যবহারযোগ্যতা যত বৃদ্ধি পাবে, এটি তত বেশি ব্যবহারকারীকে আকৃষ্ট করতে পারবে, ফলে প্রতিটি সংযোগের ক্ষেত্রে সম্ভাব্য উৎস (possible sources) ও গন্তব্য (destinations) এর পরিমাণ বৃদ্ধি পাবে এবং প্রতিটি ব্যবহারকারী আরো বেশী সিকিউরড বা নিরাপদ হবে।

২.৩. টর ব্রাউজার কনফিগারেশন

২.৩.১. ব্রীজ রীলে

যেসব টর ব্যবহারকারীদের ইন্টারনেট সার্ভিস প্রভাইডার বা দেশ প্রকাশিত টর নোডগুলোতে প্রবেশ বন্ধ করে দেয় (যেমনঃ চীন) যাতে কেউ টরের নেটওয়ার্কের সাথে সংযুক্ত হতে না পারে তাদের জন্যই ব্রীজ রীলে। ব্রীজ রীলে শুধু প্রাথমিক অবস্থায় টর নেটওয়ার্কের সাথে যুক্ত হওয়ার জন্য করা হয়।

নিরাপত্তার দিকে থেকে চিন্তা করলে লাভ এটিই হবে যে, যেহেতু ব্রীজ রীলে গুলো প্রকাশিত হয় না তাই আমরা যে টর ব্যবহার করছি এই ব্যাপারটা লুকানো যাবে। তাই যদি আপনার বসবাস এমন স্থানে হয় যেখানে টর ব্যবহার করাই সন্দেহজনক তখন ব্রীজ রীলে ব্যবহার করতে পারেন। যদিও ব্রীজ রীলে ব্যবহার করলে আপনার ব্রাউজিং গতি অনেক কমে যাবে কারণ প্রকাশিত রীলের থেকে অপ্রকাশিত রীলের ব্যন্ডউইথ সাধারণত কম থাকে।

ব্রিজ ব্যবহার করার জন্য প্রথমে আপনাকে যে কোন একটি ব্রিজ এড্রেস খুঁজে পেতে হবে। এরপর টর নিজে নিজে অন্যান্য ব্রিজ খুঁজে বের করবে। প্রথমে টর ব্রিজ এড্রেস পাওয়ার উপায় হলোঃ

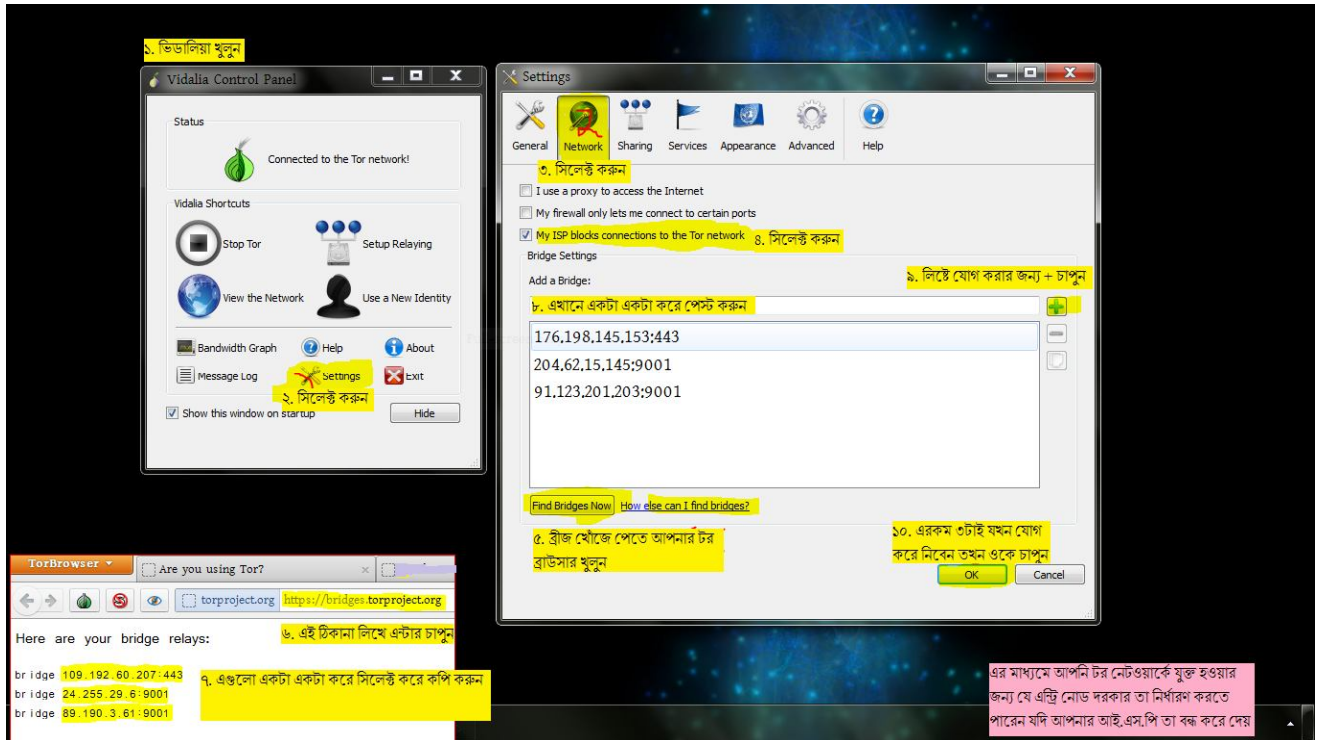
(ক) bridges.torproject.org সাইট থেকে ব্রিজ এর এড্রেস পাওয়া যাবে।

(খ) bridges@torproject.org ঠিকানায় ইমেইল করেও এটা সংগ্রহ করা যাবে। এক্ষেত্রে ইমেইলের বডিতে 'get bridges' কথাটি লিখতে হবে। আর মেইল পাঠাতে হবে gmail.com অথবা yahoo.com থেকে। আর এভাবে ইমেইলে লেটেস্ট ব্রিজ এর তালিকা সংগ্রহ করাই উত্তম।

ব্রীজ এড্রেস সংগ্রহ করার পর কিভাবে টর এর মধ্যে ব্রীজ সেটআপ করতে হবে, তা নীচে চিত্রের সাহায্যে দেখানো হলোঃ

১। টাস্কবার থেকে Vidalia Control Panel ওপেন করুন।

২। Settings সিলেক্ট করুন।

৩। Network অপশনে ক্লিক করুন।

৪। My ISP blocks connection to the Tor Network অপশনে ক্লিক করুন।

৫। ইমেইলে পাওয়া এড্রেস হতে 176.198.145.153:443 এ রকম আইপি এড্রেস ও পোর্ট নাম্বার এর জোড়া Add a Bridge এর নীচে text box এ copy-paste করুন।

৬। ডান দিকের সবুজ প্লাস চিহ্নে ক্লিক করুন।

৭। এভাবে অবশিষ্ট ২ টি এড্রেস যোগ করে দিন।

৮। সবার শেষে নীচে OK বাটনে ক্লিক করুন।

২.৩.২. প্রক্সি সার্ভার (Proxy Server)

টরের বর্তমান ভার্সন এবং Vidalia কন্ট্রোল প্যানেল HTTPS প্রক্সি সাপোর্ট করে। এতে সুবিধা এই যে, যদিও কোন এলাকার আইএসপি টর এর সকল সার্ভার ব্লক করে রাখে তবুও প্রক্সি সার্ভার এর মাধ্যমের টর ব্যবহার করা যাবে।

যদিও সাধারণ প্রক্সি সার্ভার আমাদের ডাটা গুলি দেখতে পায়, কিন্তু HTTPS প্রক্সি তা দেখতে পারবে না। এটাই HTTPS এর বৈশিষ্ট্য। এমন কি আমরা কোন সাইটে ভিজিট করছি, তাও ঐ প্রক্সি সার্ভার দেখতে পারবে না। তারা শুধু এতটুকু জানবে যে, আমরা তার মধ্য দিয়ে টর নেটওয়ার্কে প্রবেশ করছি।

এক্ষেত্রে গুরুত্বপূর্ণ হচ্ছে বেশ কয়েকটি HTTPS, SOCKS4, or SOCKS5 প্রক্সি এড্রেস জোগাড় করে রাখা। এই সাইটে দেশ অনুযায়ী প্রক্সি সার্ভার তালিকা আছেঃ http://hidemyass.com/proxy-list/

উপরের ছবিতে China এর প্রক্সিগুলো দেখা যাচ্ছে। উপরের দেশ নির্দিষ্ট করে দেয়া যায়, পরে হলুদ রঙ এর Update Results বাটনে ক্লিক করলে ঐ দেশের প্রক্সিগুলো দেখা যাবে। রেজাল্টে আইপি এড্রেস, পোর্ট ও প্রকার দেয়া আছে, এসব তথ্য দিয়ে আমরা এই প্রক্সি সার্ভারকে ব্যবহার করতে পারবো।

এছাড়া কোন প্রক্সি সার্ভারে কোন নিরাপত্তা সমস্যা আছে কিনা তা টেস্ট করার জন্যঃ http://proxy-test.zzl.org/ ভিজিট করুন।

যদি টর ব্রিজ ব্যবহার করে আপনার পর্যাপ্ত নিরাপত্তা লাভ না হয়, তাহলে আপনি প্রক্সি ব্যবহার করতে পারেন।

নীচে প্রক্সি সার্ভার কনফিগার করার পদ্ধতি দেয়া হলোঃ

১। Vidalia কন্ট্রোল প্যানেল ওপেন করুন। টাস্কবারে টর আইকনে ডাবল ক্লিক করলে যে প্যানেল উঠে আসে তাই হলো Vidalia কন্ট্রোল প্যানেল।

২। Settings সিলেক্ট করুন।

৩। Network অপশনে ক্লিক করুন।

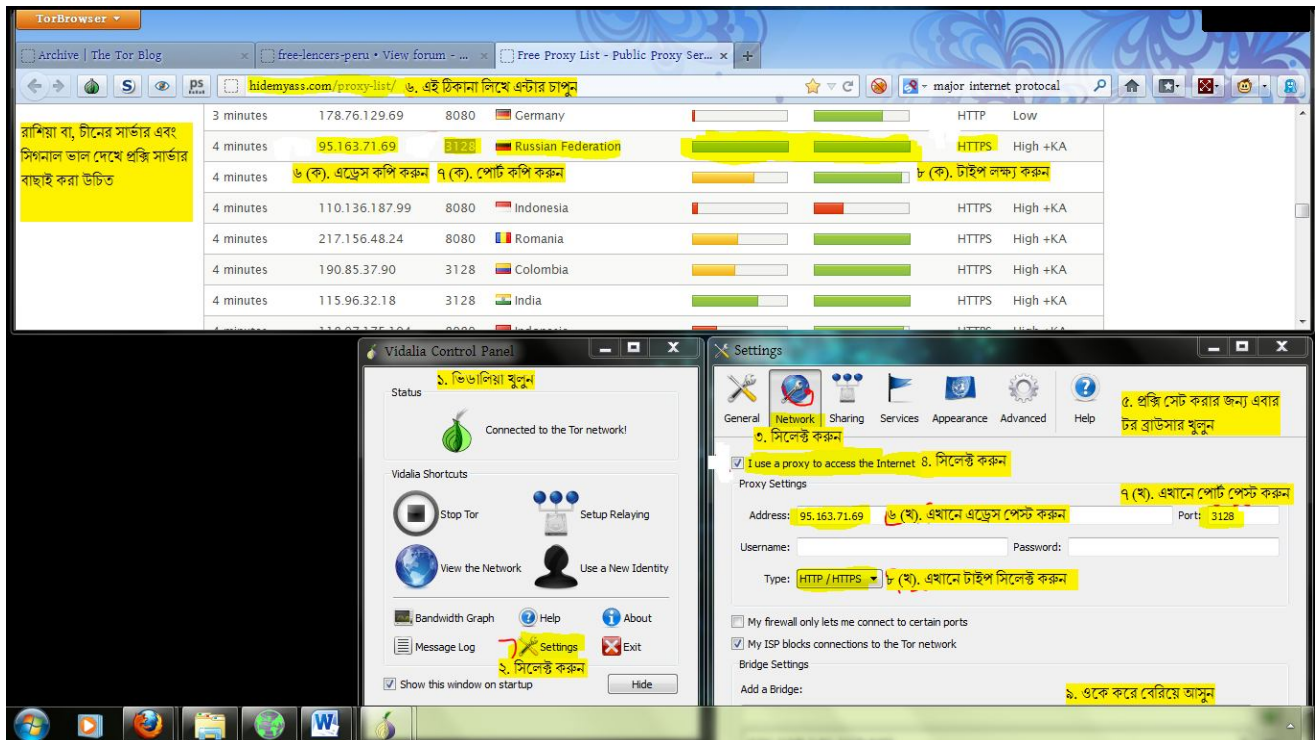
৪। তারপর 'I use a proxy to access the Internet' চেক বক্স এ টিক চিহ্ন দিন।

৫। Address এর পাশের বক্সে প্রক্সি এড্রেস অথবা hostname (ওয়েব এড্রেস) টাইপ করুন। এরপর Port নম্বর টাইপ করুন।

৬। সাধারণত username এবং password দেয়ার দরকার হবে না। দরকার হলে সে তথ্যগুলি দিন।

৭। তারপর প্রক্সি এর Type (প্রকার) নির্ধারণ করুন। যেমনঃ HTTP/HTTPS, SOCKS4, or SOCKS5. এই তথ্য প্রক্সি সার্ভারের ওয়েব পেইজ এ দেয়া থাকবে। যা উপরের সাইটেও দেয়া আছে।

৮। OK বাটনে ক্লিক করুন।

এভাবে প্রক্সি এর মাধ্যমের টর ব্যবহার হবার জন্য প্রস্তুত হয়ে গেলো।

বিঃদ্রঃ

১. আমেরিকা কিংবা কানাডার প্রক্সি ব্যবহার না করা ভালো। এগুলো থেকে কাফিররা সহজে তথ্য আদায় করতে পারে। চীন কিংবা রাশিয়া এর প্রক্সিগুলো ব্যবহার করবেন। তাতে কাফিরদের জন্য তথ্য জোগাড় করা আরো কঠিন হবে।

২. ওয়েব এড্রেস এর শেষে .ru থাকা মানে এই নয় যে এটি রাশিয়ার অবস্থিত একটি সার্ভার। বরং তা আমেরিকায়ও অবস্থিত হতে পারে। তাই সতর্কভাবে প্রক্সি সিলেক্ট করুন।

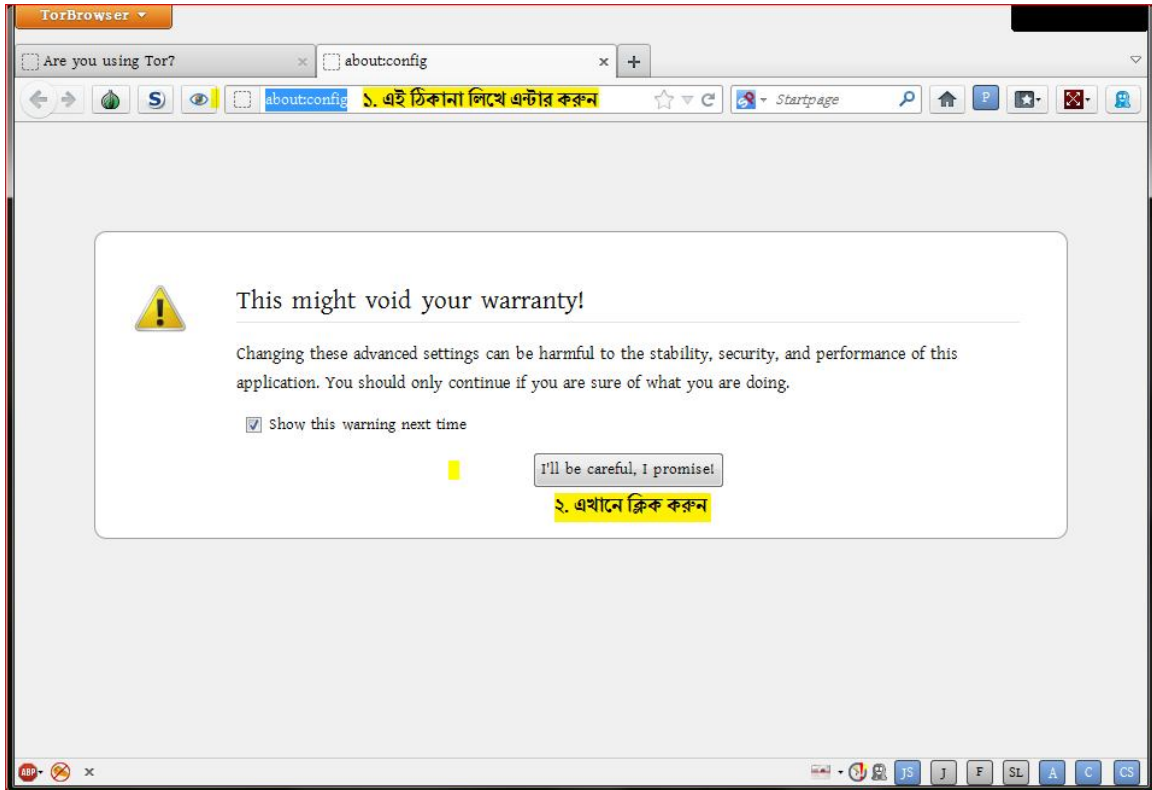
৩. http://whatismyipaddress.com/proxy-check এই সাইটের মাধ্যমে প্রক্সির কোন সমস্যা আছে কিনা, কোন তথ্য লিক করে কিনা জানা যায়। শুধু প্রক্সি এর ভিতর দিয়ে ঐ পেইজ ওপেন করলেই হবে।

৪. উল্লেখ্য সব প্রক্সি আমাদের টর এর পাঠানো ডাটা Forward করবে না। তাই প্রক্সি সেট করার পর টর চালিয়ে দেখে নিতে হবে তা ঠিকমতো কাজ করছে কি না !!!

২.৩.৩. কিছু Preference সেট করা।

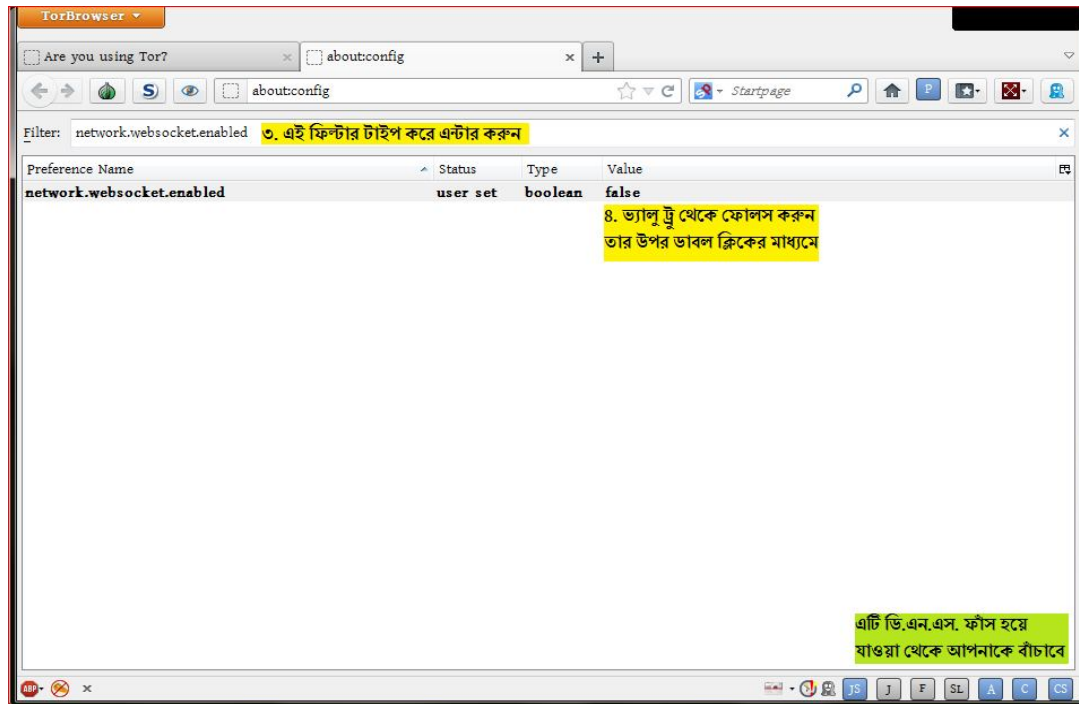
টর ব্রাউজারের গুরুত্বপূর্ণ কিছু ভেল্যু সেট করা হলো এই অধ্যায়ের উদ্দেশ্য।

ক) প্রথমে এড্রেস বারে about:config টাইপ করে, এন্টার চাপুন।

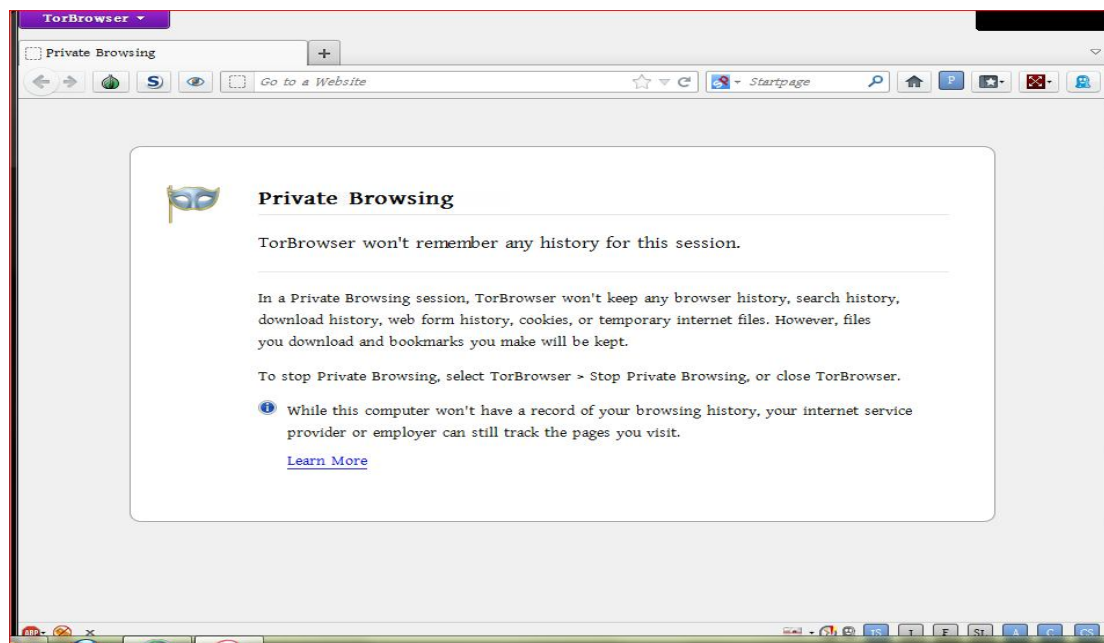
খ) I will be careful, I promise বাটনে ক্লিক করুন।

নীচের ছবির মতো বিভিন্ন ফিল্টার সার্চ করে বের করে, তাদের ভেল্যু এর উপর ডাবল ক্লিক করে ভেল্যু পরিবর্তন করুন।

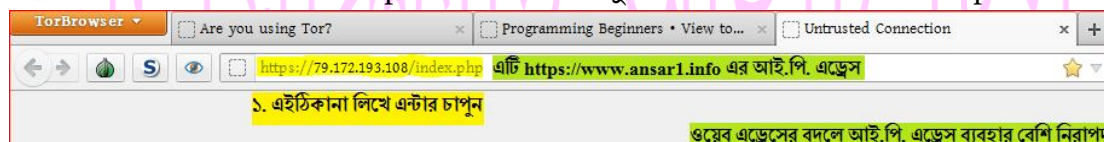
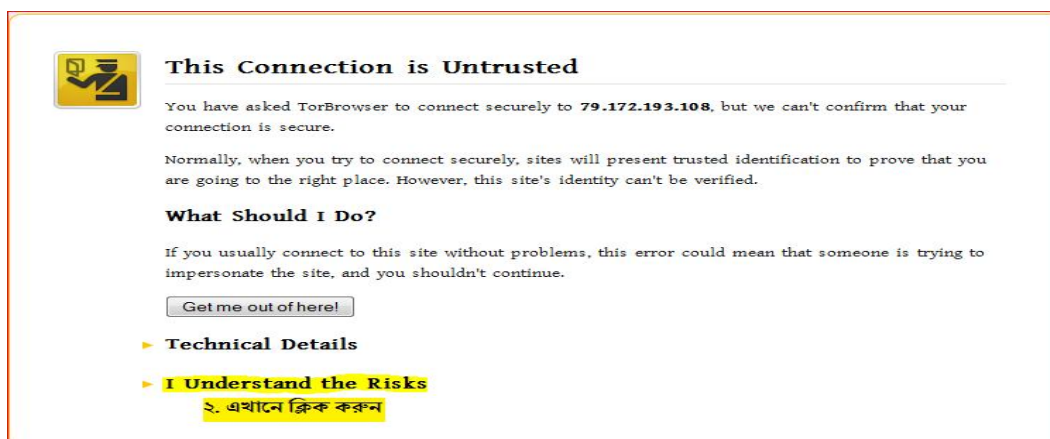
কোন সতর্কবানী দেখালে yes চাপুন

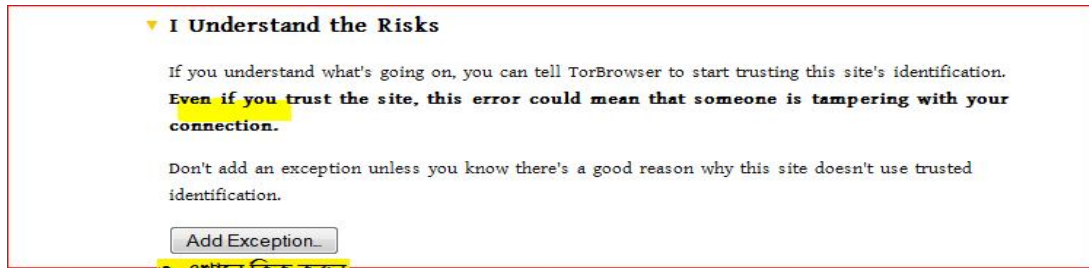
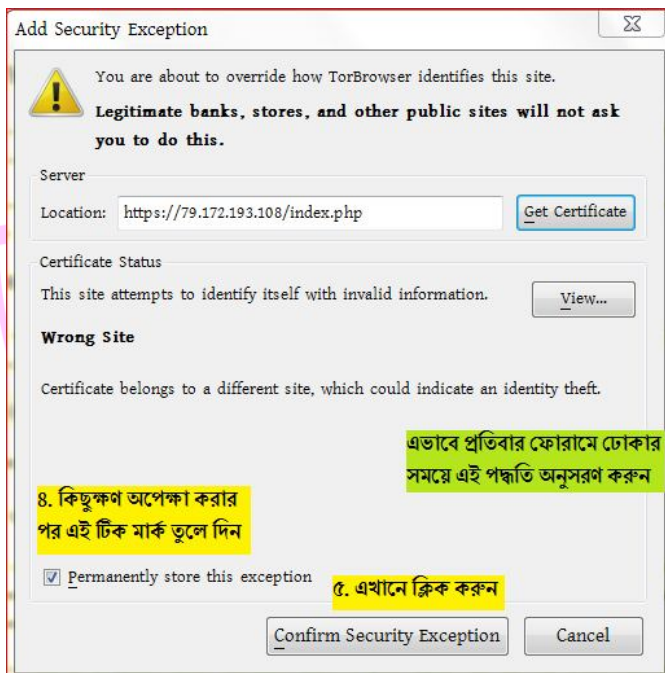
এখন সার্চ বারে নিচের Preference গুলো টাইপ করুন এবং তার ভ্যালু পরিবর্তন করুন

ফিল্টার নাম	নতুন ভ্যালু	উপকারিতা
geo.enabled	false	Geolocation disable করা
network.websocket.enabled	false	DNS leakage বন্ধ করা
geo.wifi.uri	localhost	Geolocation disable করা

২.৪. টর ব্যবহারে সতর্কতা

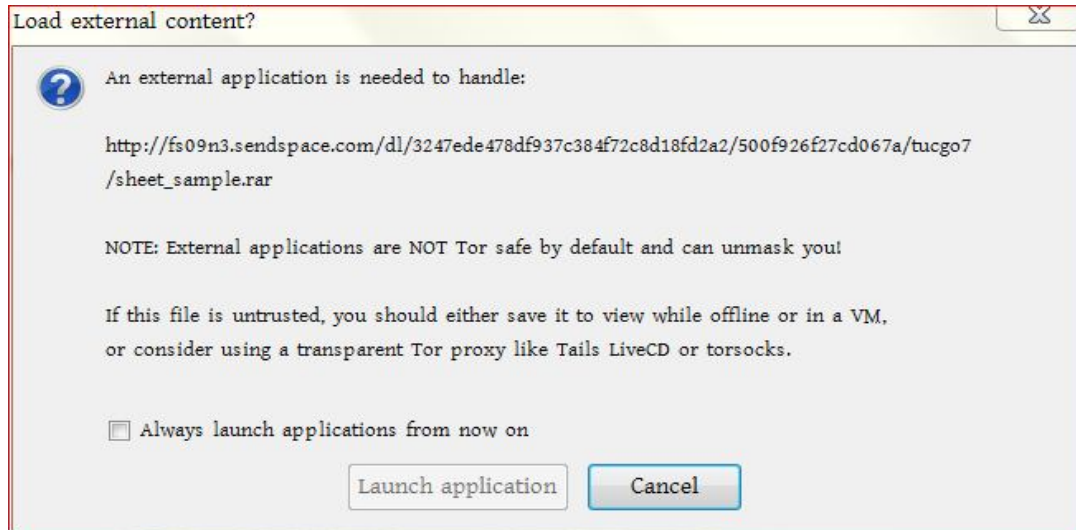
২.৪.১. প্রাইভেট সেশন

সর্বদা private session ব্যবহার করে ব্রাউজ করুন। টর ব্রাউসারে প্রাইভেট সেকশনে যাওয়ার শর্টকাটঃ Ctrl+Shift+P

২.৪.২. ওয়েবসাইটের সার্টিফিকেট অনুমোদন

যে কোন ফোরামের সার্টিফিকেট Accept করার সময় শুধু ঐ সেশনের জন্য তা Accept করুন।

যেমনঃ https://79.172.193.108 এড্রেসে ভিজিট করলে দেখবেন প্রথমবার Untrusted বলবে। তার মানে এই সাইটের সার্টিফিকেট আমাদের ব্রাউসারে রক্ষিত নেই।

তখন I Understand the Risks এ ক্লিক করতে হবে।

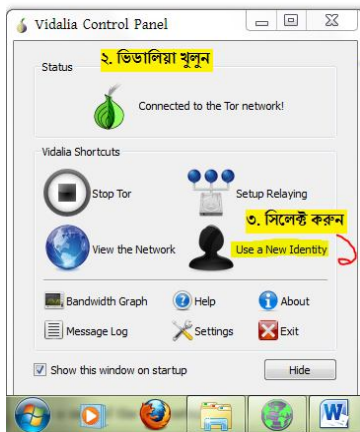
এরপর Add Exceptions বাটনে ক্লিক করতে হবে।

এরপর Permanently store this exception এর পাশে টিক মার্ক তুলে দিতে হবে।

এভাবে সাময়িকভাবে কোন সাইটের সার্টিফিকেট গ্রহণ করা হলো।

২.৪.৩. ফাইল সংরক্ষণে (Save) করণীয়

Tor এর ভিতর কোন ফাইল ডাউনলোড করার সময় নীচের ওয়ার্ণিং দিবে। তখন কোন ফাইল টরের ভিতর থেকে open করবেন না বরং তা save করুন।

এর জন্য Launch appilication এ ক্লিক করুন। এরপর অপশন আসলে Open ক্লিক না করে Save ক্লিক করুন। তাহলে সেই ফাইল সেইভ হয়ে যাবে।

কোন কোন ফাইলে ছবি কিংবা এমন কোন আইটেম থাকে যা ওপেন করলে সেই ছবি ইন্টারনেট থেকে ডাউনলোড করে নেয়। টর আমাদেরকে এই ব্যাপারে ওয়ার্ণিং দেয়।

২.৪.৪. আই.পি. পরিবর্তন

প্রত্যেক আলাদা ইমেইল আই.ডি. ব্যবহার করার জন্য অথবা নতুন কোন সাইটে গেলে আলাদা আইপি এড্রেস ব্যবহার করুন। এর জন্য নীচের ছবির মতো Vidalia Control Panel এর Use a New Identity বাটনে ক্লিক করুন।

উল্লেখ্য আইপি এড্রেস পরিবর্তন হয়েছে কিনা পরীক্ষা করার জন্য www.whatismyip.com ভিজিট করুন। অর্থাৎ আইপি পরিবর্তনের আগে এবং পড়ে ঐ সাইট থেকে আপনার আইপি এড্রেস দেখলে বুঝতে পারবেন আইপি এড্রেস পরিবর্তন হয়েছে কিনা। আপনি যে আইপি এড্রেস দেখছেন সেটা আসলে আপনার না, বরং সেটা আসলে সর্বশেষ (৩য়) Tor Relay Server এর।

২.৪.৫. ওয়েবসাইটের https ভার্সন ব্যবহার

ফোরাম সমূহে লগ-ইন করার জন্য সর্বদা SSL / https ব্যবহার করুন। যেমনঃ
http://www.ansar1.info/ এর পরিবর্তে https://www.ansar1.info/

কারণ http ব্যবহার করলে মাঝখানের যে কোন সার্ভার থেকে চাইলে আপনার লগইন আইডি, পাসওয়ার্ড দেখতে পারবে। কিন্তু https এ সেটা অনেক কঠিন।

২.৪.৬. ওয়েব এড্রেস ব্যবহার না করে সাইটের আইপি এড্রেস ব্যবহার করুন

যেমনঃ https://www.ansar1.info/ এর পরিবর্তে https://79.172.193.108 ব্যবহার করুন।

কারণ চাইলে কেউ ডিএনএস সার্ভার থেকে কেউ জানতে পারবে আপনি কোন কোন সাইটে বেশী ভিজিট করেন। কিন্তু সরাসরি আইপি এড্রেস ব্যবহার করলে ডিএনএস সার্ভার ব্যবহার হচ্ছে না।

বিঃদ্রঃ

১. টর সংযোগ হবার পর আই.পি চেক করুন। টরের ভিতরে এবং টরের বাইরে অন্য যে কোন ব্রাউজার দিয়ে।

২. অপ্রয়োজনে টর ব্যবহার না করে, সাধারণ ব্রাউজিং এর সময় (যেমন পত্রিকা পড়ার সময়) টর ব্যবহার করবেন না। পারলে অন্যান্য সাধারণ সফটওয়্যার কিংবা সাধারণ কোন আইটেম টর ছাড়াই ডাউনলোড করুন, যাতে বিভিন্ন সার্ভার থেকে আপনার ডাটা আপলোড / ডাউনলোড হয়।

২.৫. প্রক্সিফাইয়ার

আমরা যে Vidalia ব্রাউজার (টর ব্যবহার উপযোগী মজিলা ফায়ার ফক্স) ব্যবহার করি, এখন পর্যন্ত শুধু তা দিয়েই টর নেটওয়ার্কের ভিতর দিয়ে ব্রাউজ করেছি। কিন্তু আমাদের ইন্টারনেট এক্সপ্লোরার, বিভিন্ন ডাউনলোডার (আইডিএম, টরেন্ট ডাউনলোডার), বিভিন্ন মেসেঞ্জার (ইয়াহু, এমএসএন), স্কাইপি, পিডজিন, হিডেন আপলোড ও ডাউনলোড (এন্টিভাইরাস ও উইন্ডোজ আপডেট) কিংবা অন্যান্য সফটওয়্যার যেগুলি ইন্টারনেট ব্যবহার করে, সেগুলি কিন্তু সরাসরি ইন্টারনেট ব্যবহার করেছে, টর নেটওয়ার্ক ছাড়াই।

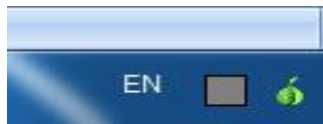
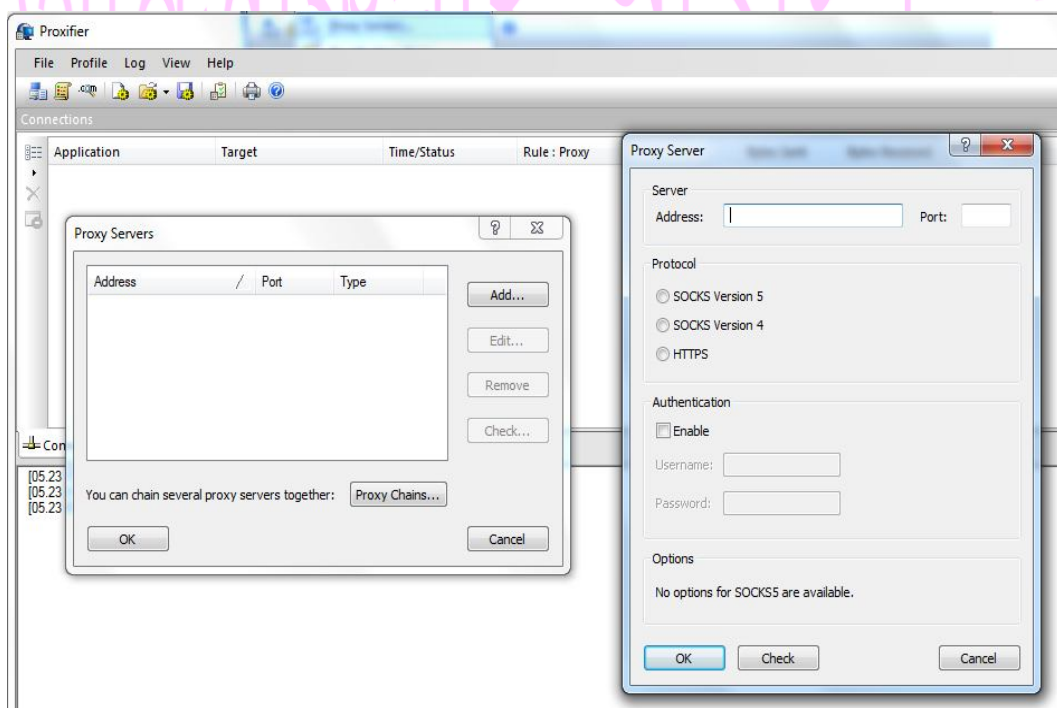
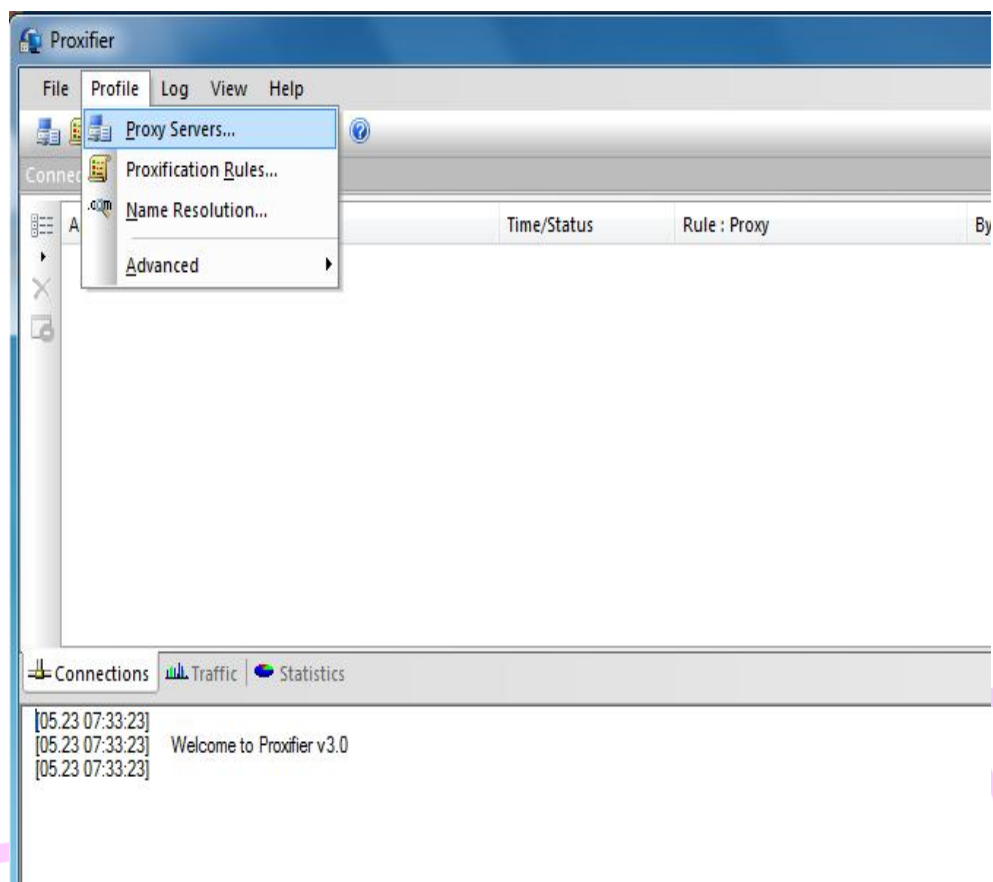
আমরা যদি আমাদের অন্যান্য সফটওয়্যারকে টরের মাধ্যমে ইন্টারনেট সংযোগ দিতে চাই, তাহলে Proxifier v3.0 নামক সফটওয়্যার ব্যবহার করতে হবে। এটা গুগল এ সার্চ দিলে সহজেই ডাউনলোড করতে পারবেন। download Proxifier v3.0 লিখে সার্চ দিলে অনেক লিংক বের হবে। এছাড়াও নীচের লিংকে Proxifier v3.0 সফটওয়্যারটি ও এর উপর একটি ভিডিও টিউটোরিয়াল আছে। http://speedy.sh/aJbSR/Pr-fi.rar

২.৫.১. প্রক্সিফাইয়ার কনফিগারেশন

এক্ষেত্রে Tor Vidalia Stable version ব্যবহার করতে হবে (এটাই আমরা সাধারণত ব্যবহার করি)।

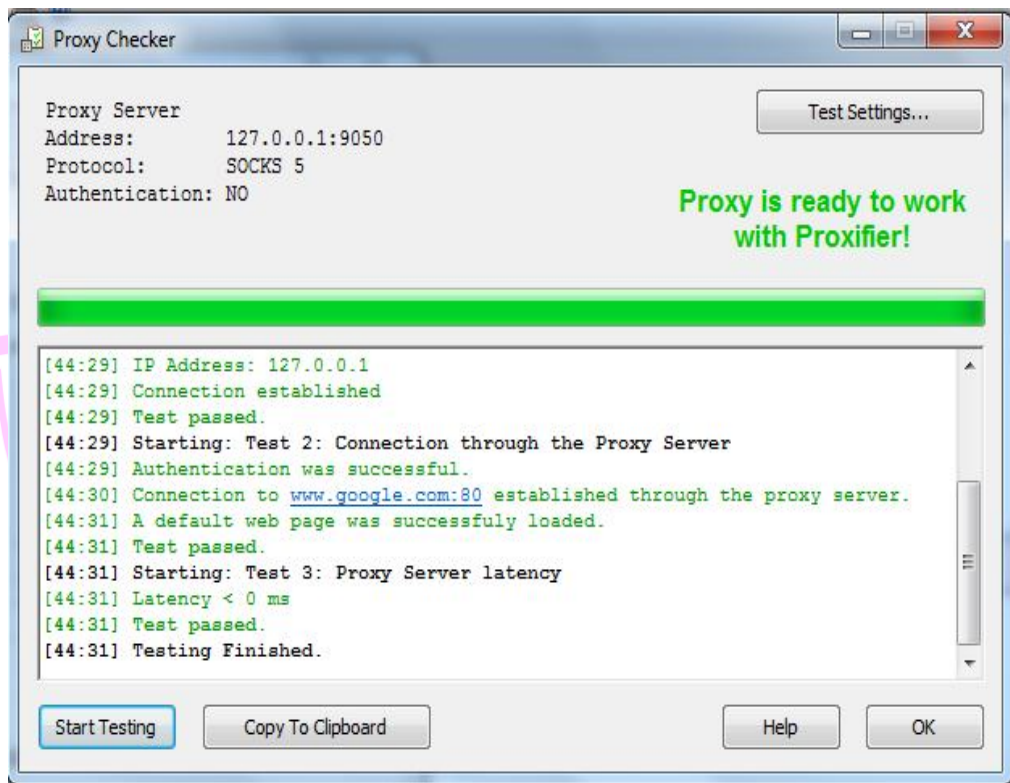
ক) প্রথমে টর এরপর Proxifier ইন্সটল করুন। (টর আগে থেকে ইন্সটল থাকলে সমস্যা নেই)

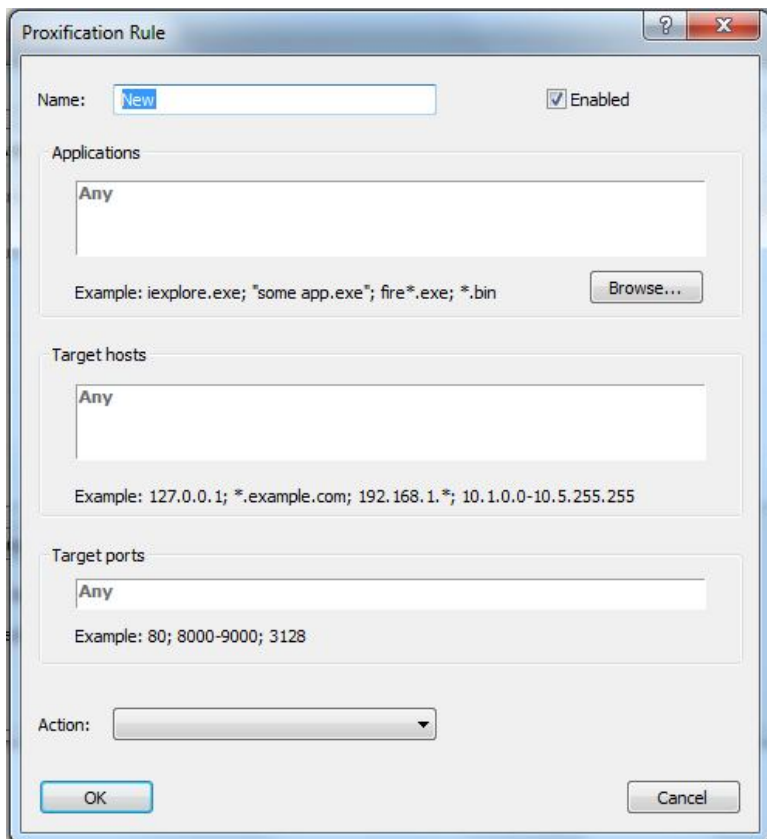
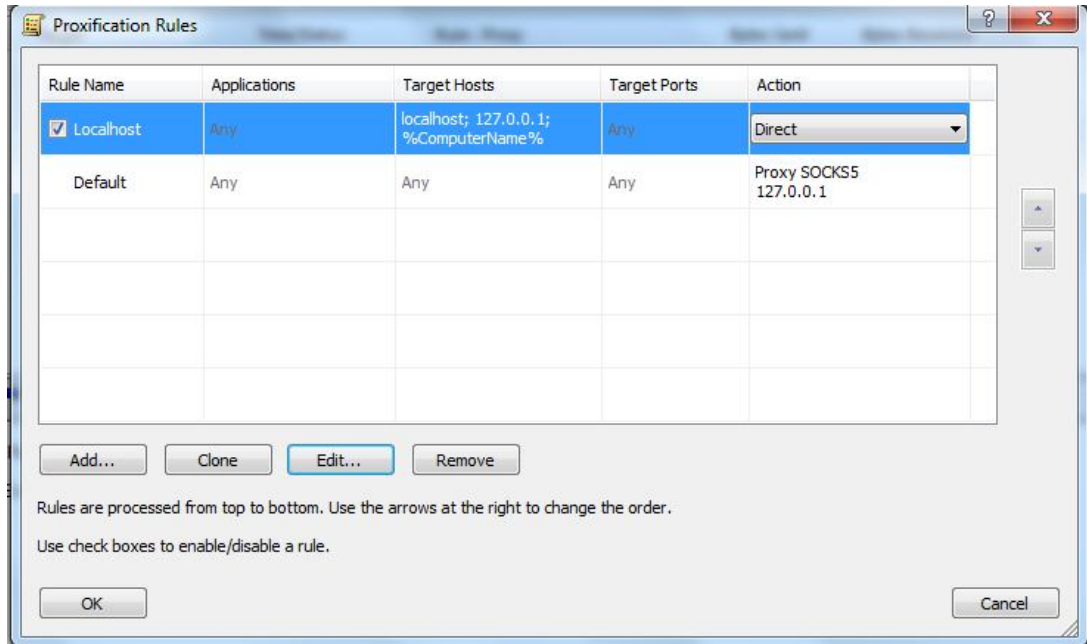
খ) টর নেটওয়ার্কে কানেক্ট করুন। (টর সফটওয়্যার চালু করুন) এবং

গ) proxifier ওপেন করুন। সেটা নটিফিকেশন এলাকায় (স্ক্রীণের নীচে ডানে দিকে) আইকন আকারে চালু হয়।

সেটাতে ডাবল ক্লিক করে তার প্যানেল চালু করুন। এখন Profile - Proxy Server এ ক্লিক করুন।

Add বাটনে ক্লিক করলে ডানের প্যানেল আসবে। Address: হিসেবে 127.0.0.1 এবং Port এ 9050 লিখুন। টর ডাটা আদান-প্রদানের জন্য এই পোর্ট ব্যবহার করে।

Protocol হিসেবে Socks Version 5 সিলেক্ট করুন। তারপর নীচে Check বাটনে ক্লিক করে দেখে নিন তা কাজ করছে কি না। তারপর OK বাটনে ক্লিক করুন।

তারপর OK বাটনে ক্লিক করুন।

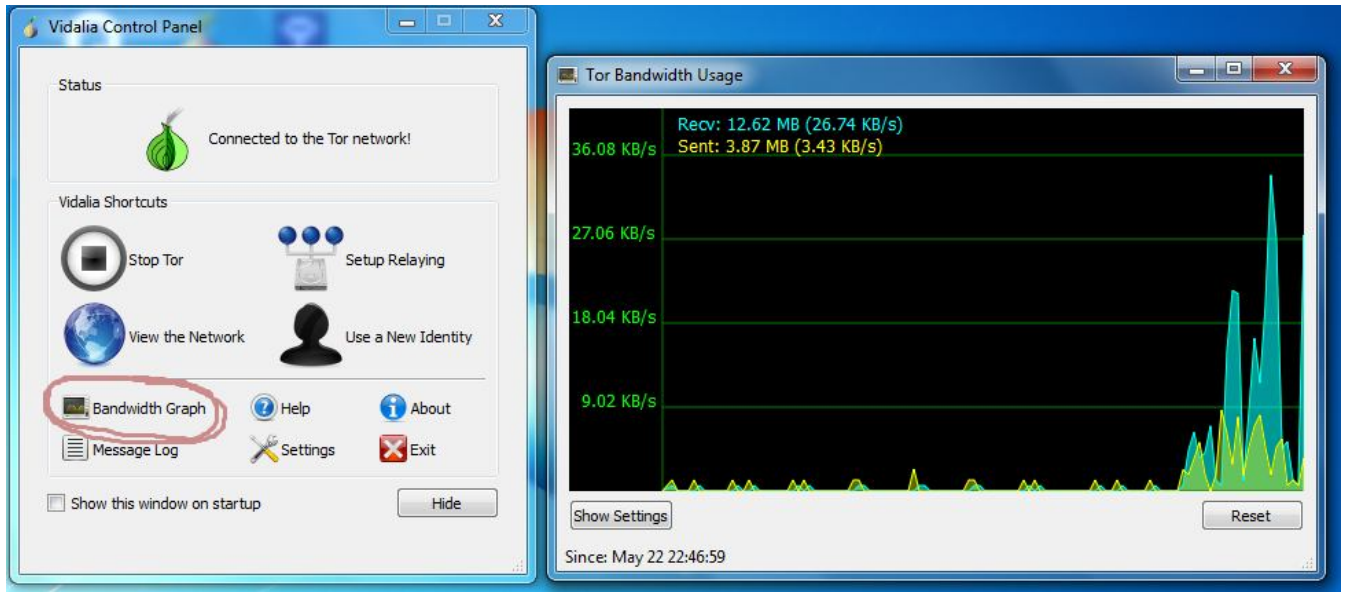
এরপর Proxifier ঠিকমতো কাজ করছে কিনা পরীক্ষা করার জন্য Check বাটনে ক্লিক করুন।

২.৫.২. প্রক্সিফাইয়ারে অন্যান্য সফটওয়্যার যোগ করার পদ্ধতিঃ

এরপর মেন্যু থেকে Profile - Proxification Rules এ ক্লিক করুন। Add বাটনে ক্লিক করুন।

প্যানেলের Name হিসেবে Internet Explorer লিখুন। Applications এর Browse বাটনে ক্লিক করে C:\Program Files\Internet Explorer সিলেক্ট করুন। নীচে Actions হিসেবে Proxy Socks5 127.0.0.1 সিলেক্ট করুন। OK বাটনে ক্লিক করুন।

এরপর Proxification Rules এর OK বাটনে ক্লিক করুন।

২.৫.৩. প্রক্সিফাইয়ারে টেস্টিং

এখন টরের ভিতরে (ফায়ারফক্সে) এবং টর এর বাইরে ইন্টারনেট এক্সপ্লোরারে www.whatismyip.com ভিজিট করলে দেখবেন, দুই পেইজেই একই আইপি এড্রেস দেখাচ্ছে। কারণ ইন্টারনেট এক্সপ্লোরারে এখন টরের ভিতর দিয়ে কাজ করছে। এভাবে যে কোন ডাউনলোড সফটওয়্যার, মেসেঞ্জার ইত্যাদিও সেট করা যাবে।

প্রমাণ হিসেবে ইন্টারনেট এক্সপ্লোরারে চালানোর সময় Vidalia Control Panel এর Bandwidth Graph দেখুন, দেখবেন তখনও টরের ভিতর দিয়ে ডাটা যাচ্ছে।

উল্লেখ্য টর কেবলমাত্র TCP streams (transmission control protocol) এর জন্য কাজ করে এবং তা যে কোন এপ্লিকেশান দ্বারা ব্যবহার করা যাবে যদি ওইসব এপ্লিকেশান SOCKS support করে। এ কারণে যে সব প্রোগ্রাম TCP/IP প্রটোকল ব্যবহার করে না, সেগুলি টর এর ভিতর দিয়ে চালানো যাবে না। যেমনঃ ping কিংবা tracert এসব প্রোগ্রাম TCP/IP ব্যবহার করে না। তাই এগুলো টর দিয়ে চালানো যাবে না।

২.৬. প্রায়ই যেসব প্রশ্ন করা হয়

প্রশ্নঃ টর নেটওয়ার্কে যুক্ত হওয়ার পর প্রথম সার্ভার থেকে আমাদের তথ্য প্রবাহ কি দেখা যাবে?

উত্তরঃ টর ব্যবহার করার সময় তিনটি সার্ভারের মধ্যে প্রথম সার্ভার আপনার কম্পিউটার এর আইপি দেখতে পারে। কিন্তু সে জানে না টর ব্যবহার করে আপনি কি করছেন। সে শুধু দেখতে পারে একটি নির্দিষ্ট I.P. (আপনার আইপি) টর ব্যবহার করছে। পৃথিবীর কোন জায়গায়ই টর ব্যবহার অবৈধ নয়, তাই টর ব্যবহার করায় কোন সমস্যা নেই।

প্রশ্নঃ টর নেটওয়ার্কে যুক্ত হওয়ার পর তৃতীয় সার্ভার থেকে আমাদের তথ্য প্রবাহ কি দেখা যাবে?

উত্তরঃ টর ব্যবহার করার সময় তিনটি সার্ভারের মধ্যে তৃতীয় সার্ভারটি আপনার তথ্য দেখতে পারে তবে তা কোন কম্পিউটার থেকে পাঠানো হচ্ছে তা দেখতে পায় না। আর যদি আপনি https ব্যবহার করে, তবে সে ভিতরের তথ্যও দেখতে পারে না। শুধু এতটুকু দেখতে পারে যেঃ www.ansar1.info তে কেউ একজন ভিজিট করছে। অর্থাৎ https ব্যবহার করলে তৃতীয় সার্ভারটি শুধু আমাদের গন্তব্য দেখতে পাবে কিন্তু তথ্য-প্রবাহের ভিতরের তথ্য সে দেখতে পাবে না। তাই তখনও আপনি নিরাপদ কারণ সে জানতে পারবে না আপনি কে কিংবা আপনার আইপি এড্রেস কি?

প্রশ্নঃ টর ব্রীজ কি এটা লুকিয়ে রাখতে পারে যে আপনি টর ব্যবহার করছেন?

উত্তরঃ সাধারণত এটা আপনাকে লুকিয়ে রাখতে পারবে, তবে খুব অল্প সম্ভাবনা আছে আপনার প্রকাশিত হয়ে যাবার। আপনার ISP যদি খুব চালাক হয় এবং যদি সে সকল টর ব্রীজ এর আইপি বের করতে পারে তবে হয়ত আপনি যে টর ব্যবহার করছেন তা তারা বুঝতে পারে। কিন্তু টর ব্যবহার করে তো আপনি গুগল কিংবা অন্য কোন সাইটেও যেতে পারেন। আর কোন আইএসপি এর এতদূর যাবার সম্ভাবনা খুবই কম।

প্রশ্নঃ টর ব্রীজের উপর কি আপনার ব্রাউজিং স্পীড নির্ভর করে?

উত্তরঃ হ্যাঁ। এটা খুবই স্বাভাবিক। ব্রীজ থেকে ব্রীজ কানেকশান পার্থক্য হয়। যেমন ধরুন, আমি ব্রীজ রান করছি। এখন আমার ভিতর দিয়ে যারা কানেকশান নেবে, স্বাভাবিকভাবেই তারা স্লো কানেকশান পাবে। আবার মনে করুন, এমন একজন ব্রীজ রান করাচ্ছে যার স্পীড খুব বেশী, যখন কেউ সেই ব্রীজের ভিতর দিয়ে যাবে, তখন সে খুব ফাষ্ট কানেকশান পাবে। তাই অনেক ক্ষেত্রে আপনাকে ব্রীজ বদলিয়ে দেখতে হবে কোনটাতে ভালো কানেকশান পাচ্ছেন।

প্রশ্নঃ আমরা টর ব্রাউজারের হোম পেইজে কোন আইপি দেখি? এক্সিট নোড না এন্ট্রি নোড?

উত্তরঃ এক্সিট নোড।

প্রশ্নঃ এন্ট্রি নোডটা কি পাবলিক নেটওয়ার্কের কেউ বুঝতে পারে?

উত্তরঃ না, তবে তা অসম্ভব না। এটা বুঝতে পারা খুব কঠিন ব্যাপার। আপনার আইএসপি এটা বুঝতে পারে। যদি কখনো আইএসপিগুলো সরকারের চাপে টর ব্যবহার করতে না দেয় তখন টর ব্রীজ বা প্রক্সির ব্যবহার করা যাবে।

প্রশ্নঃ লোকাল হোস্ট কি?

উত্তরঃ লোকাল হোস্ট মানে হচ্ছে আপনার নিজের কম্পিউটার যার আইপি এড্রেস হচ্ছে ১২৭.০.০.১

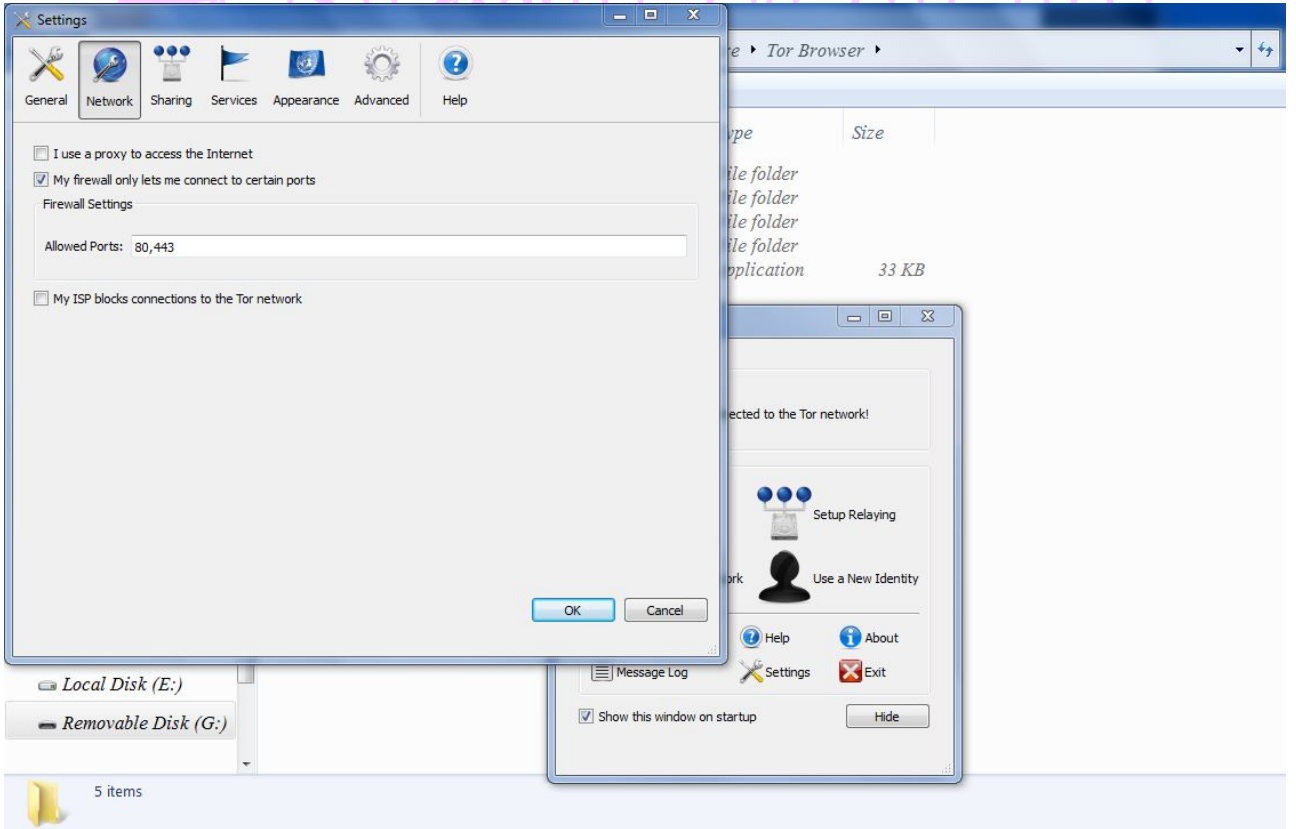
প্রশ্নঃ প্রক্সিফায়ার ১২৭.০.০.১ দিয়ে কি করে?

উত্তরঃ প্রক্সিফায়ার আপনার পিসি (১২৭.০.০.১) কে প্রক্সি সার্ভার হিসেবে ব্যবহার করে আর সেটা আবার টর এর ৯০৫০ পোর্ট নাম্বার দিয়ে আপনার ডাটা পাঠায়। এভাবে টর এর ভিতর দিয়ে সকল প্রোগ্রাম চালানো হয়।

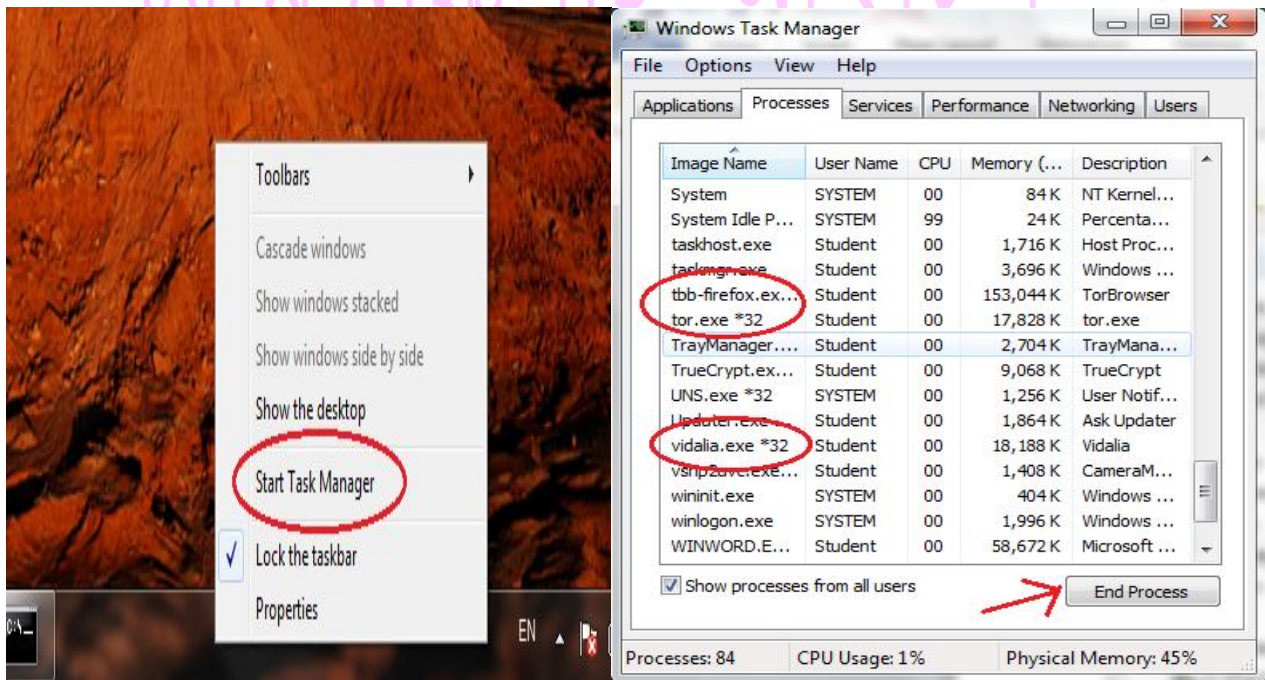
২.৭. ট্রাবলশুটিং

অনেক সময় টর ব্রাউজার ঠিকমতো কাজ করে না কিংবা রান করে না। হতে পারে নীচের কোন কারণে আপনার টর ব্রাউজার কাজ করছে নাঃ

২.৭.১. সিস্টেম ক্লক সংক্রান্তঃ আপনার system clock টি বন্ধ রয়েছেঃ আপনি এটা নিশ্চিত করুন যে আপনার system সঠিক সময় ও দিন-ক্ষণ দিচ্ছে। অতঃপর পুনরায় টর restart দিন। আপনার system clock কে Internet time server এর সাথে synchronize (একই সময়ে নিয়ে আসা) করতে হতে পারে।

২.৭.২. ফায়ারওয়্যাল সংক্রান্তঃ আপনাকে হয়ত কোনো firewall প্রতিহত করছে। আপনি এমনভাবে টর সেটআপ করুন যেন তা শুধুমাত্র port 80 এবং port 443 ব্যবহার করে। প্রথমে Vidalia control panel এ যান এবং Settings এ click করুন, অতঃপর Network এ click করুন এবং Network ট্যাবে যান তারপর My firewall only lets me connect to certain ports নামক বাক্সে tick করুন।

হতে পারে আপনার anti-virus program টরকে ব্লক করে দিচ্ছেঃ এটা নিশ্চিত করুন যে আপনার anti-virus program টর কে সংযোগ স্থাপন করতে বাধা দিচ্ছে না।

২.৭.৩. টর নেটওয়ার্কে সংযোগ বন্ধ করে দিলেঃ যদি তারপরও টর কাজ না করে, তাহলে এটা হতে পারে যে আপনার Internet Service Provider (ISP) টর কে ব্লক করে দিচ্ছে। এক্ষেত্রে আপনি টর ব্রীজ (Tor bridges) বা hidden relays ব্যবহার করতে পারেন যা সহজে ব্লক করা যায় না।

২.৭.৪. আগে থেকে চলা টর ব্রাউসারঃ এমনও হতে পারে আগে থেকে কোন টর ব্রাউজার চলছে তাই নতুন টর চালু হচ্ছে না। Tor bundle ওপেন করার আগে task manager ওপেন করুন। task manager ওপেন করার জন্য আপনার taskbar-এ রাইট ক্লিক কোরে task manager অপশনে ক্লিক করুন। এখানে list of processes-এ দেখুন যে Vidalia অথবা tbb-firefox এখনোও চলছে কিনা। যদি দেখেন যে, কোনটি এখনোও চলছে, তাহলে সেটি সিলেক্ট কোরে End process ক্লিক করুন। সাহায্যের জন্য নীচের ছবিটি দেখতে পারেন।

এরপর Tor/Vidalia bundle আবার স্টার্ট করুন আর Vidalia আপনা-আপনি ব্রাউজার ওপেন করবে, যদি কানেকশন তৈরী করতে সে সক্ষম হয়।

৩. সফটওয়্যার

৩.১. যেসব সফটওয়্যার ব্যবহার করতে হবে

৩.১.১. যে কোন একটি ভালো 'ফায়ারওয়াল' ব্যবহার করুন। যেমনঃ Zone Alarm কিংবা Comodo ইত্যাদি।

৩.১.২. সাধারণ ব্যবহারের সময় ইন্টারনেট এক্সপ্লোরার ব্যবহার পরিত্যাগ করুন। এটা uninstall করুন। ফায়ারফক্স কিংবা ওপেরা ব্রাউজার ব্যবহার করুন।

৩.১.৩. বিভিন্ন গুরুত্বপূর্ণ ফাইল Eraser কিংবা এ জাতীয় সফটওয়ারের মাধ্যমে safe delete করুন।

৩.২. যেসব সফটওয়্যার বর্জন করতে হবে

PDF ফাইল পড়ার জন্য Adobe Reader ব্যবহার করবেন না বরং Foxit Reader কিংবা এ জাতীয় সফটওয়্যার ব্যবহার করুন।

Internet Explorer বর্জন করুন। এটা নিরাপদ নয়। এর পরিবর্তে Firefox, Mozilla ইত্যাদি ব্রাউজার ব্যবহার করুন।

৪. আসরার আল মুজাহিদীন সফটওয়্যার ব্যবহার

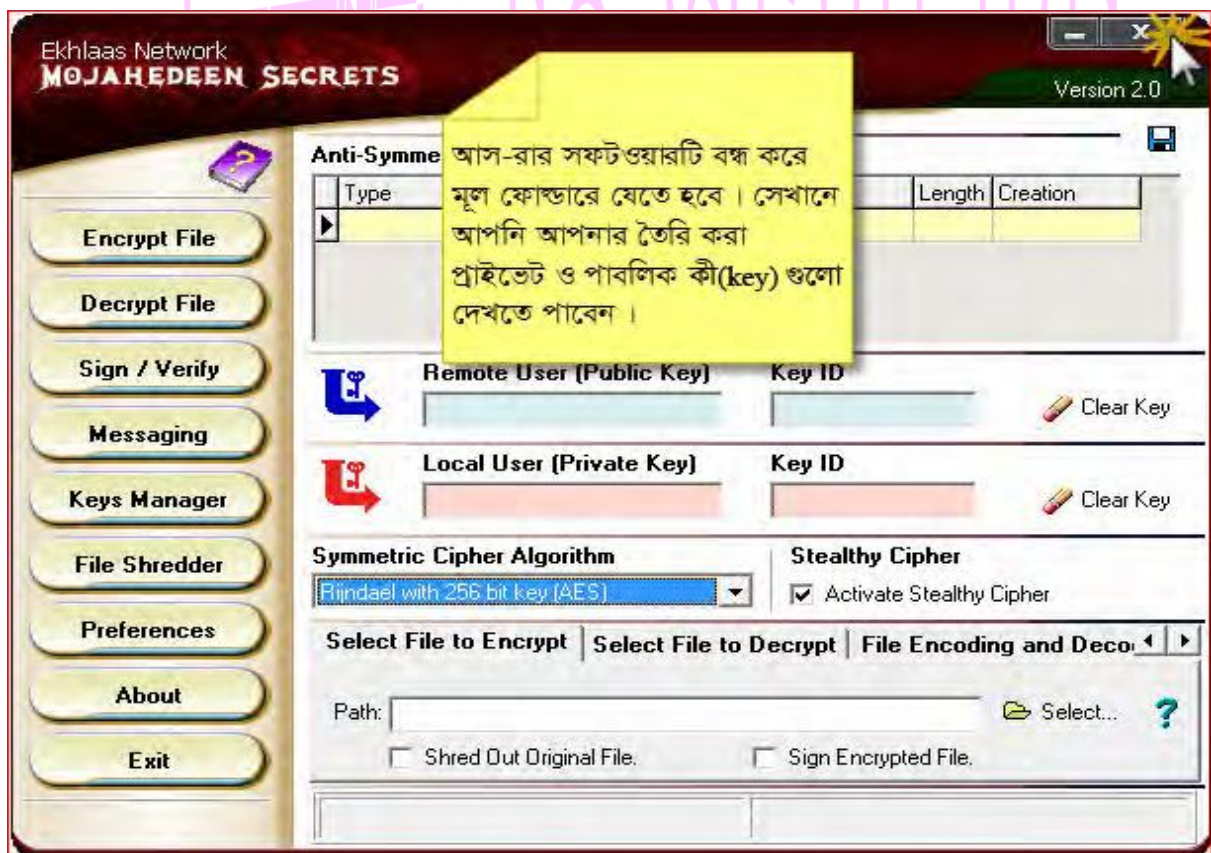
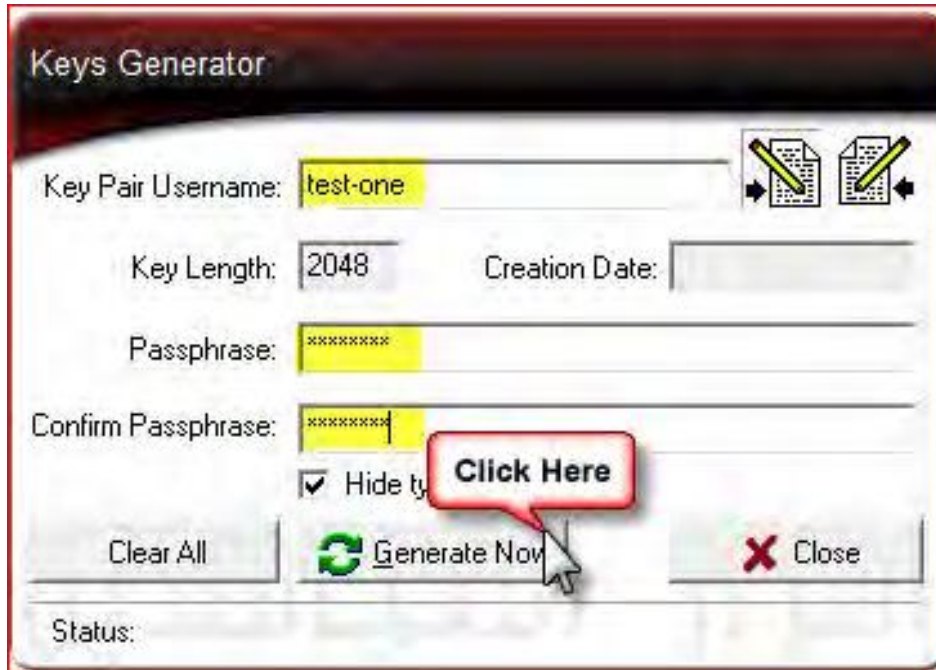
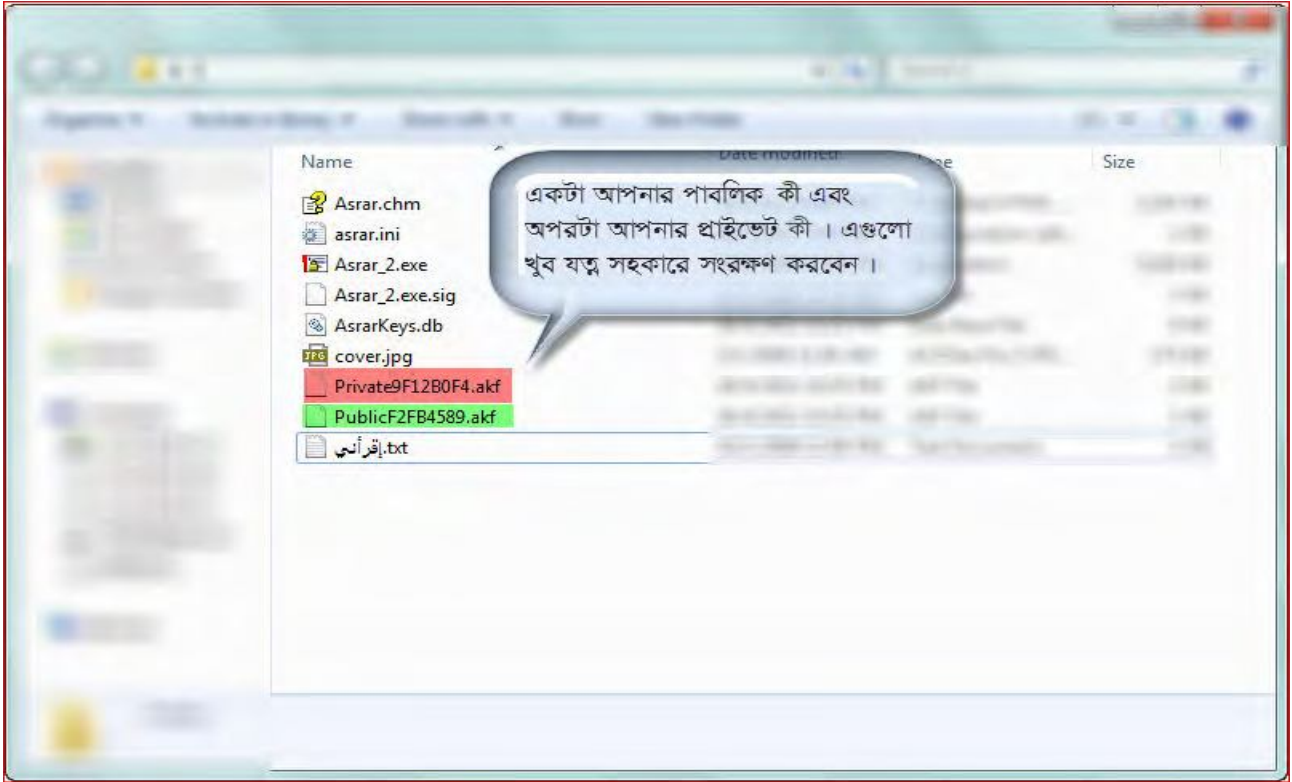
জরুরী ও গুরুত্বপূর্ণ মেসেজ আদান-প্রদানে আসরার আল মুজাহিদীন সফটওয়্যার ব্যবহার করুন।

৪.১. প্রাইভেট ও পাবলিক কী তৈরির পদ্ধতি

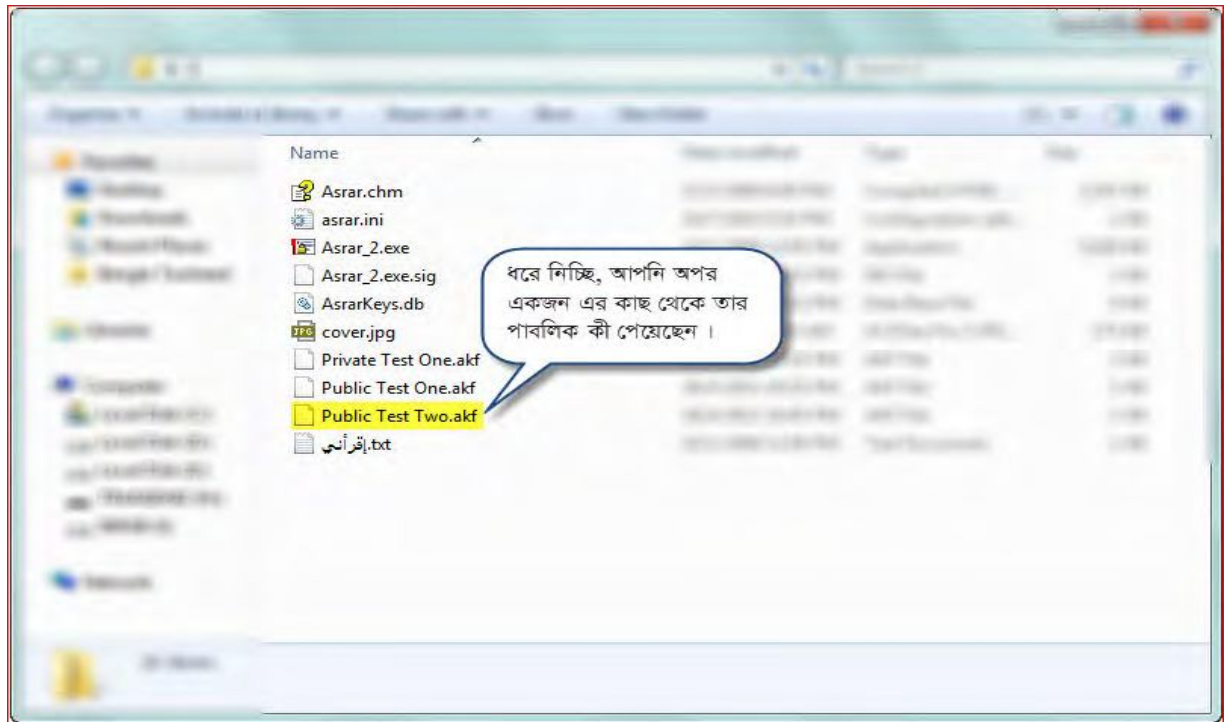
প্রথমে Keys Manager ক্লিক করুন।

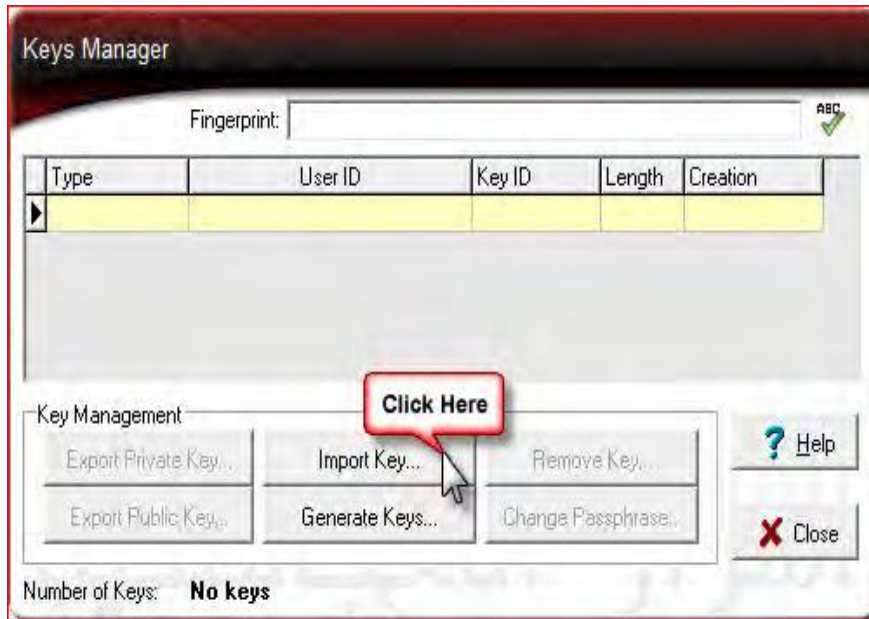
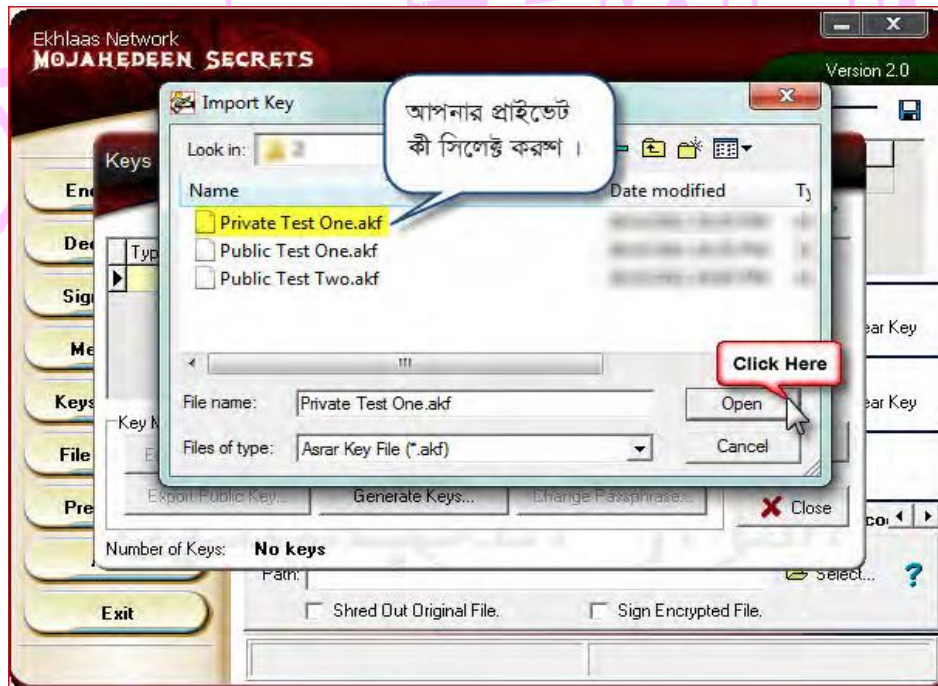
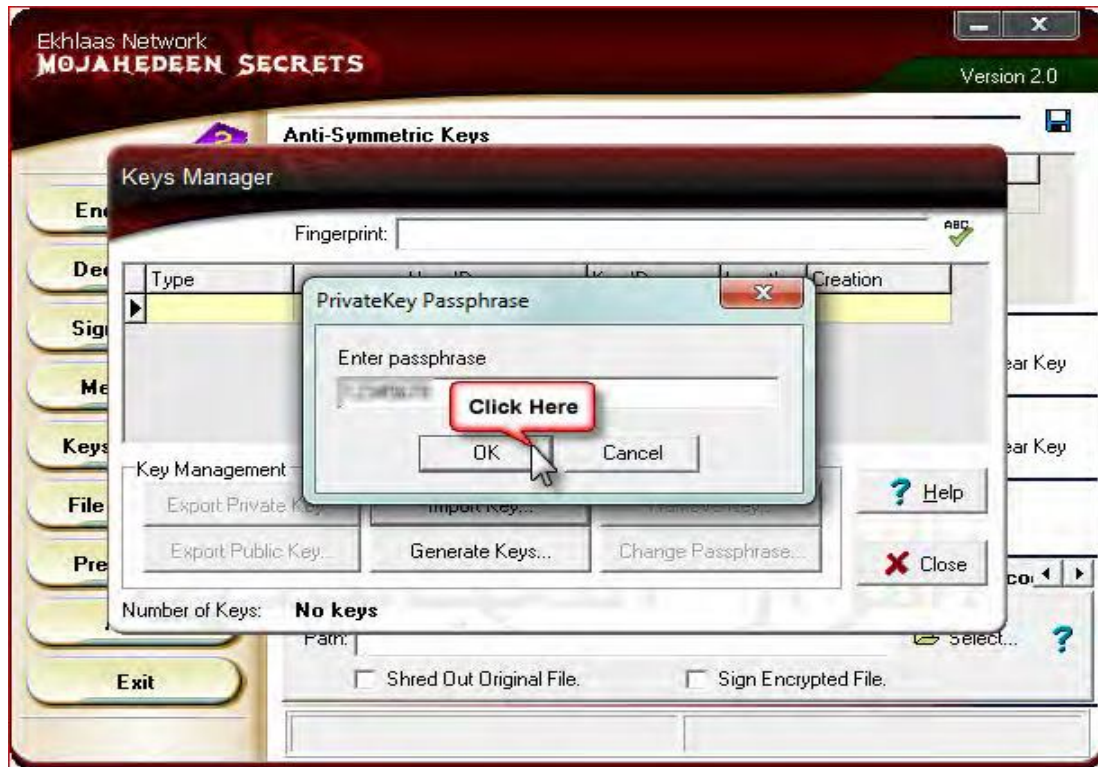
নিজের প্রাইভেট কী তৈরীর জন্য Generate Keys বাটনে ক্লিক করুন।

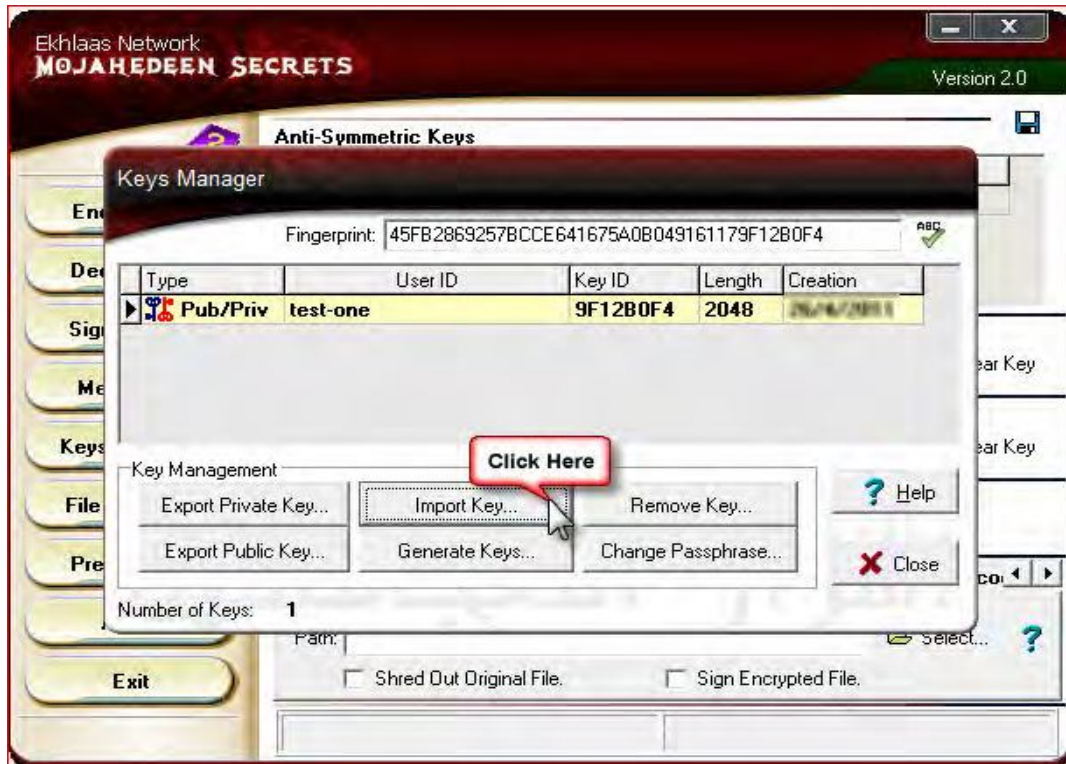
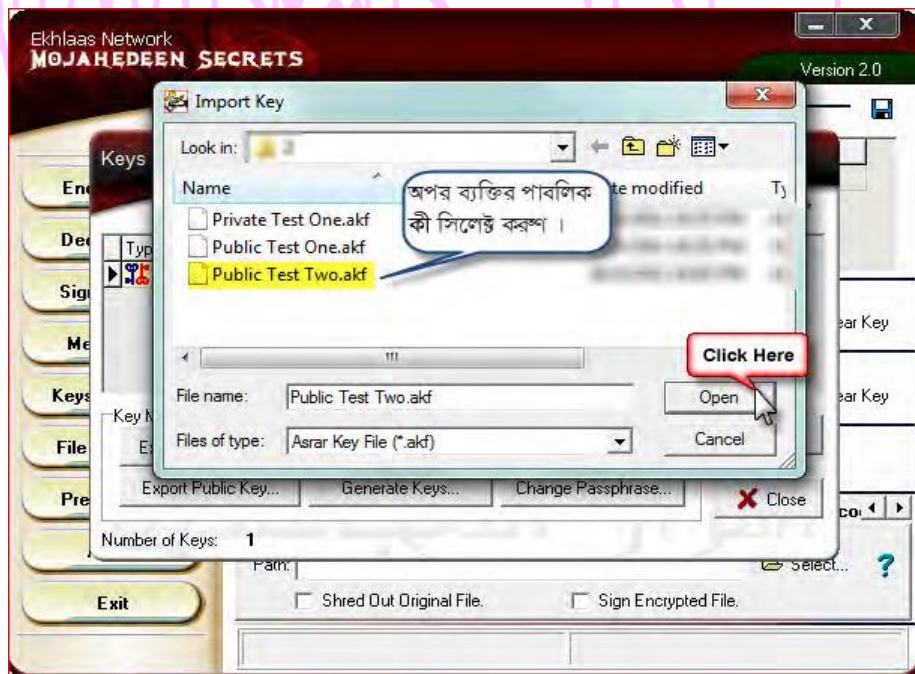
একটা ইউজার নেম ও পাসওয়ার্ড সেট করুন। যে কোন মেসেজ পড়তে এই পাসওয়ার্ড লাগবে।

এরপর Generate Now বাটনে ক্লিক করুন। কী তৈরী হয়ে গেলে Close বাটনে ক্লিক করে বের হয়ে যান।

এখন যে ফোল্ডারে আসরার সফটওয়্যার আছে সেই ফোল্ডারে আপনার পাবলিক ও প্রাইভেট কী তৈরী হয়েছে। আপনার পাবলিক কী rename করুন। (যেমনঃ abdullah.akf) আপনার বন্ধু / ভাইদের কাছে পাঠিয়ে দিন।

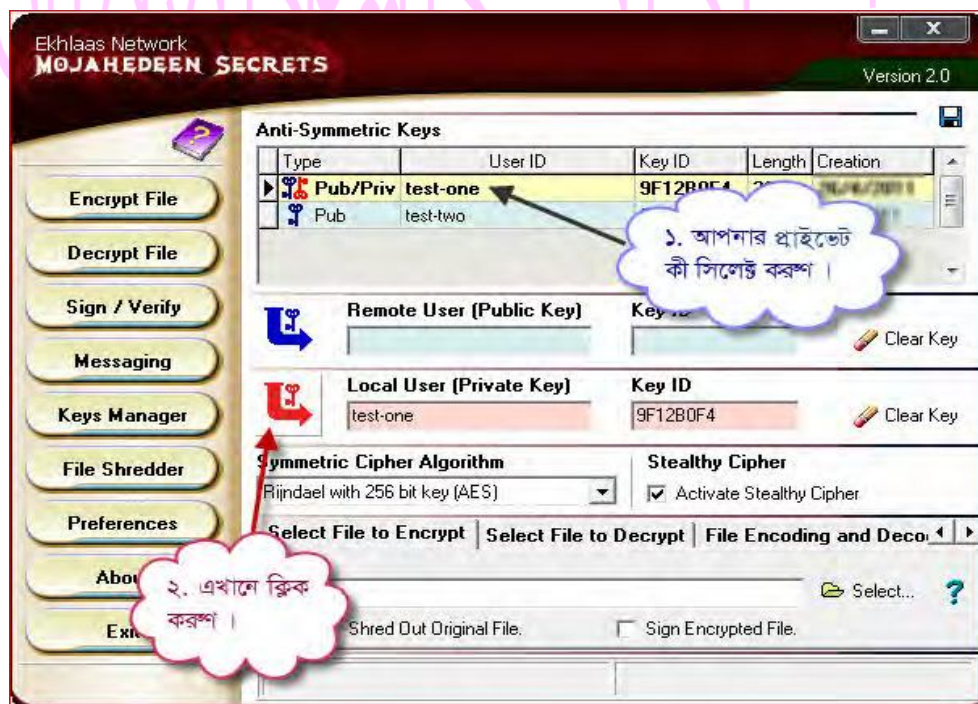
আবার আপনার কোন বন্ধুর / ভাই এর পাবলিক কী আপনাকে পাঠিয়ে থাকলে সেটা ব্যবহার করার আগে আপনাকে সেই কী ইমপোর্ট করতে হবে। এর জন্য আগের মতো Keys Manager ওপেন করুন। এরপর Import Keys ক্লিক করে আপনার প্রয়োজনীয় কী গুলি ইমপোর্ট করুন।

৪.২. প্রাইভেট এ পাবলিক কী ইমপোর্ট করার পদ্ধতি

আবার Key Manager ওপেন করুন।

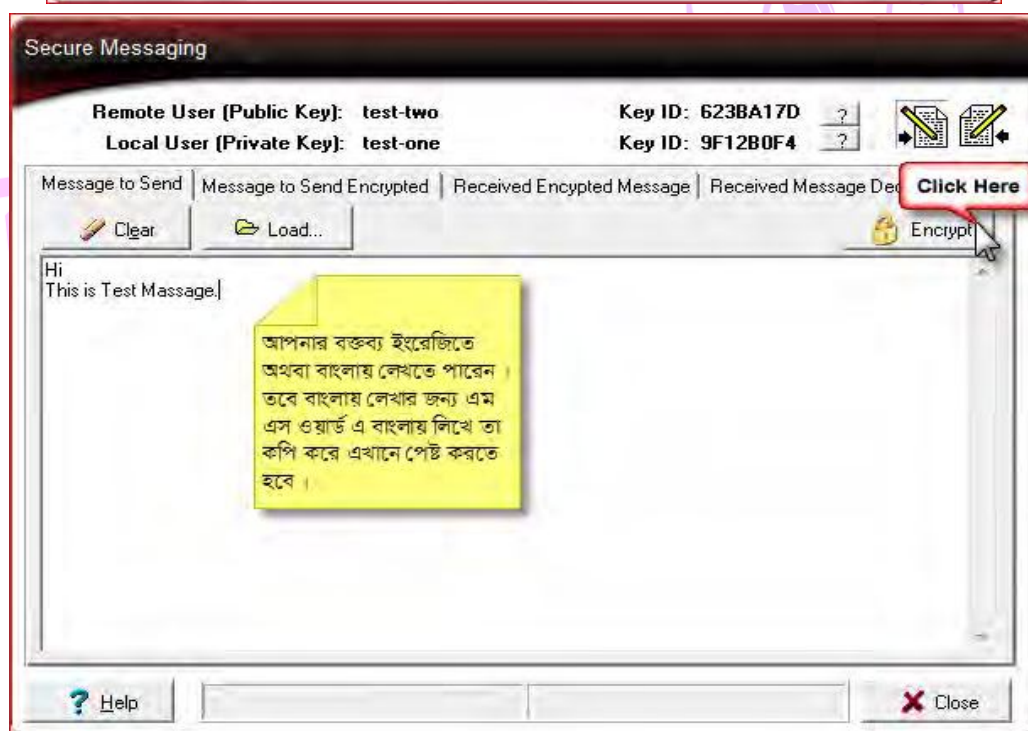
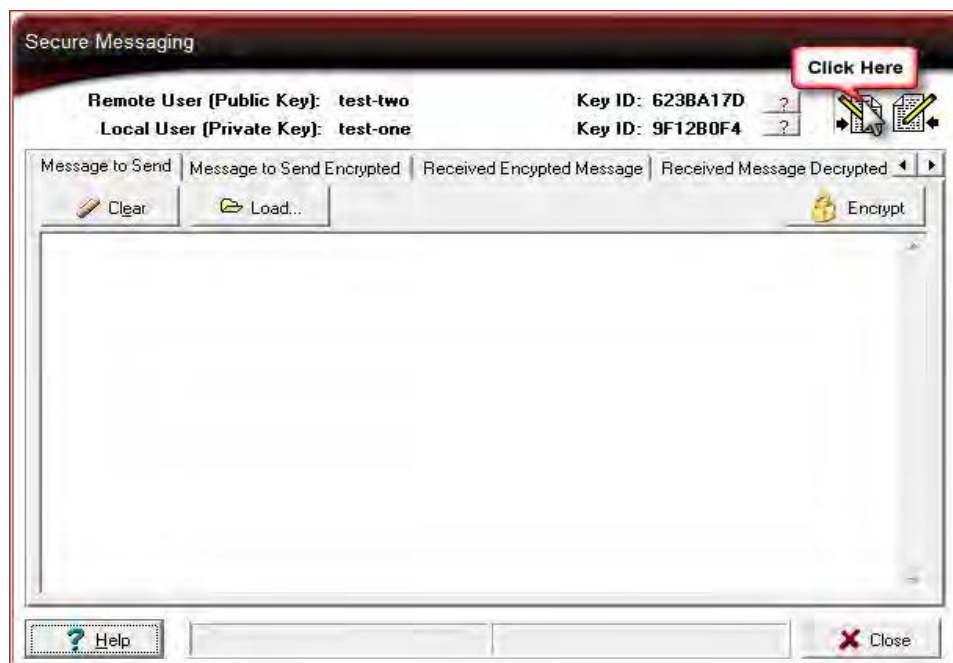
Import Keys বাটনে ক্লিক করুন।

প্রথমে আপনার নিজের প্রাইভেট কী ইমপোর্ট করার জন্য আপনার প্রাইভেট কী সিলেক্ট করুন।

পাসওয়ার্ড চাইলে পাসওয়ার্ড দিয়ে দিন। (প্রাইভেট ও পাবলিক কী তৈরী করার সময় যে পাসওয়ার্ড দিয়েছিলেন সেটা)

এখন Key Manager এ আপনার প্রাইভেট কী দেখা যাবে।

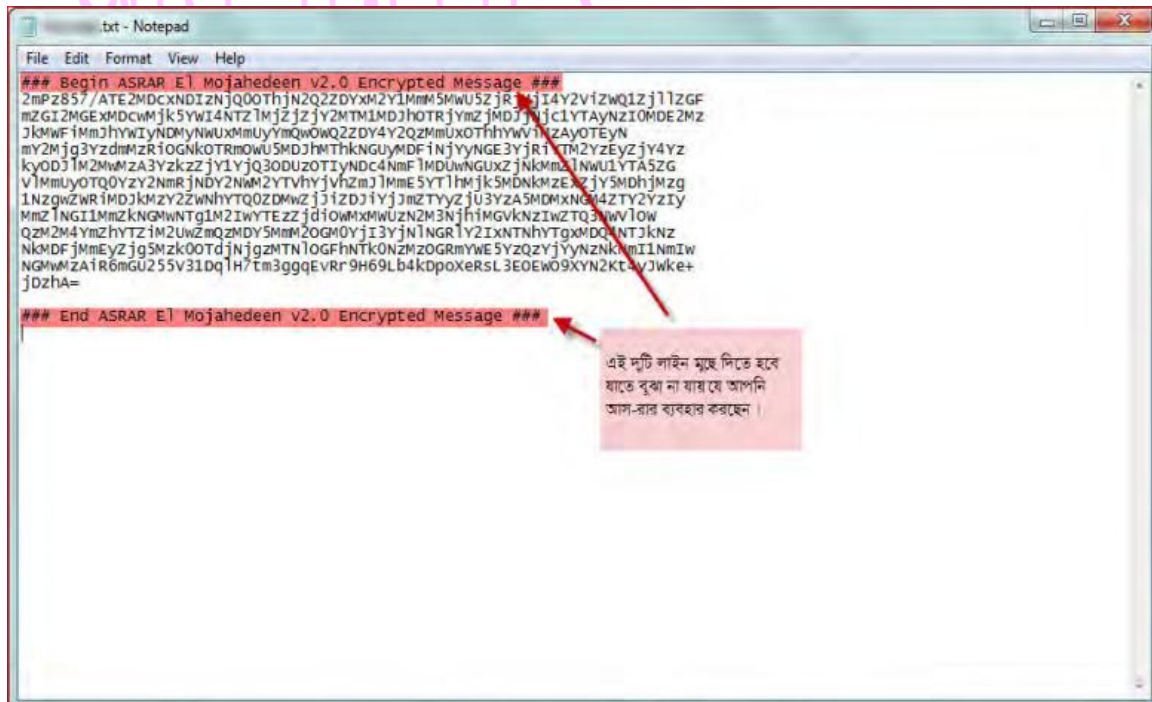
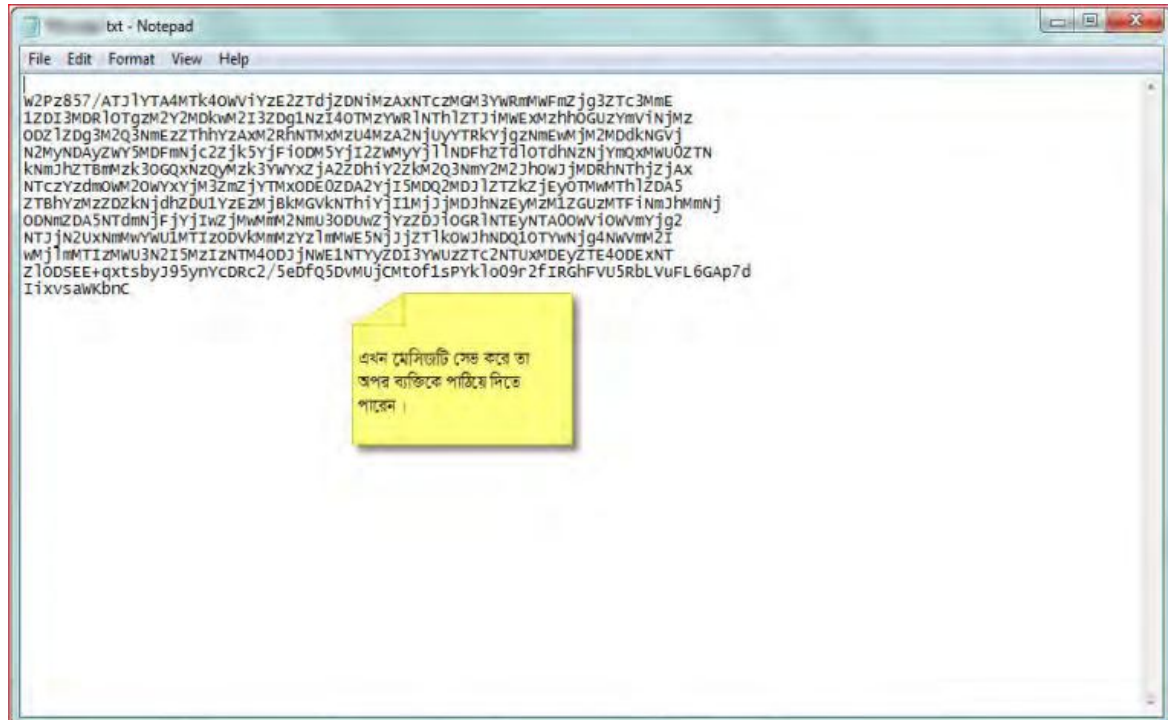
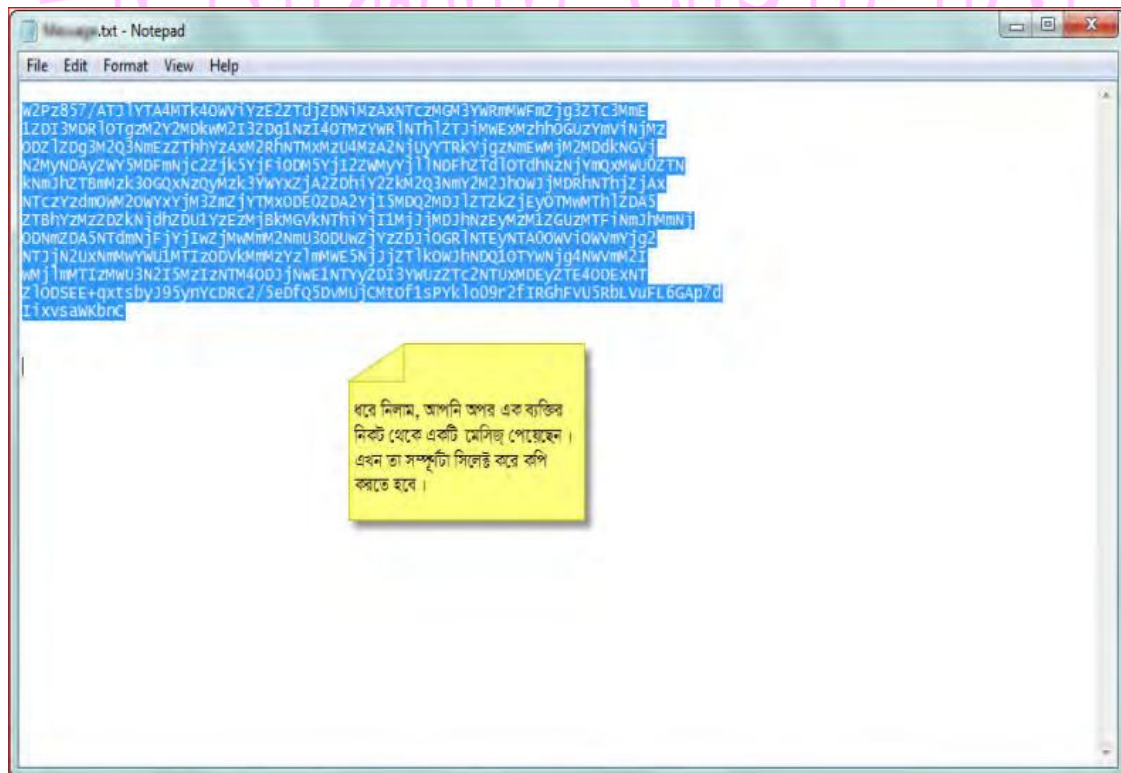
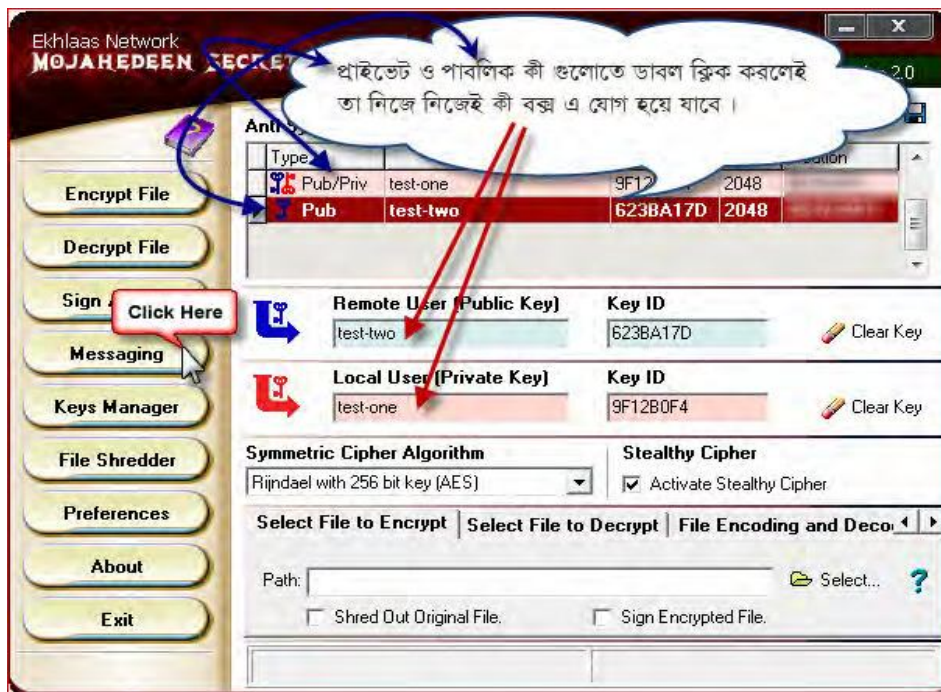
এখন আপনার বন্ধুর পাবলিক কী ইমপোর্ট করার জন্য আবার Import Key চাপুন।

আপনার বন্ধু পাবলিক কী সিলেক্ট করুন।

এখন Key Manager এ আপনার বন্ধুর public key দেখা যাবে।

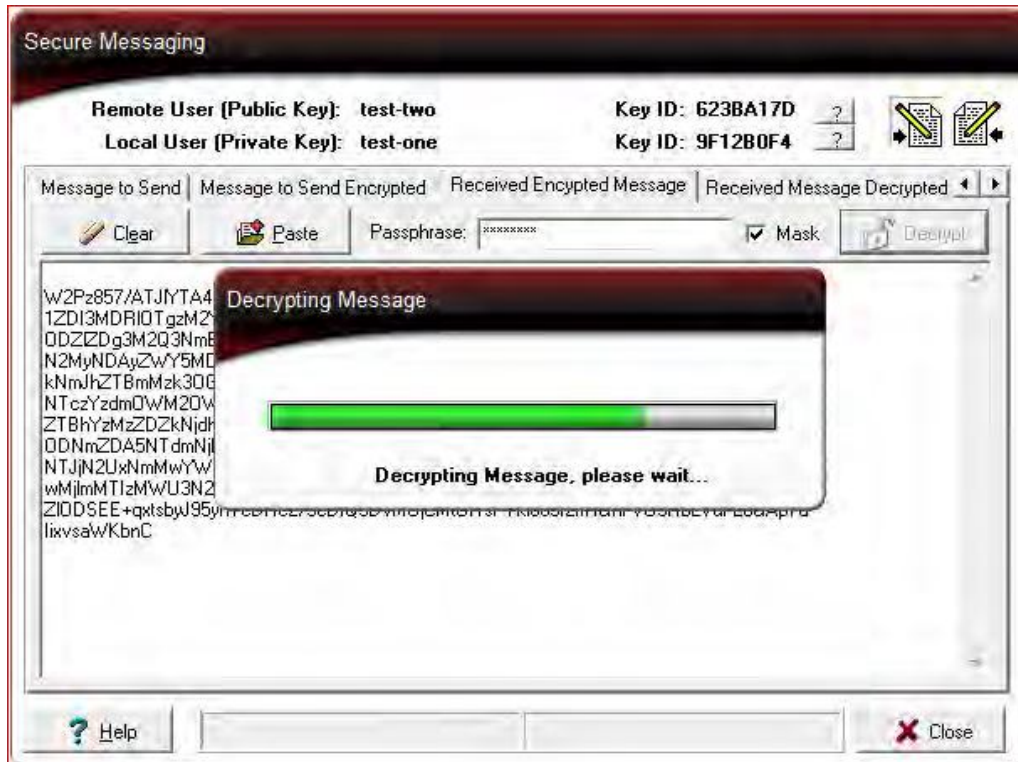
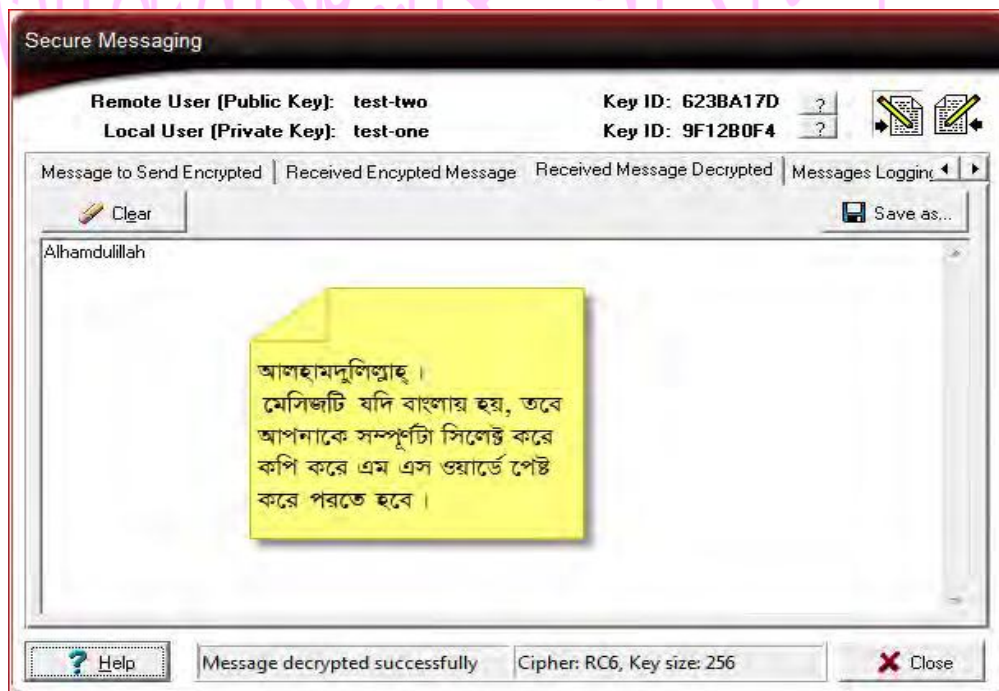
৪.৩. বার্তা এনক্রিপ্ট করার পদ্ধতি

প্রথমে আপনার প্রাইভেট কী সিলেক্ট করুন। এর উপর ডাবল ক্লিক করুন।

এরপর আপনার বন্ধুর প্রাইভেট কী সিলেক্ট করুন।

এরপর বামের মেন্যু থেকে Messaging বাটনে ক্লিক করুন।

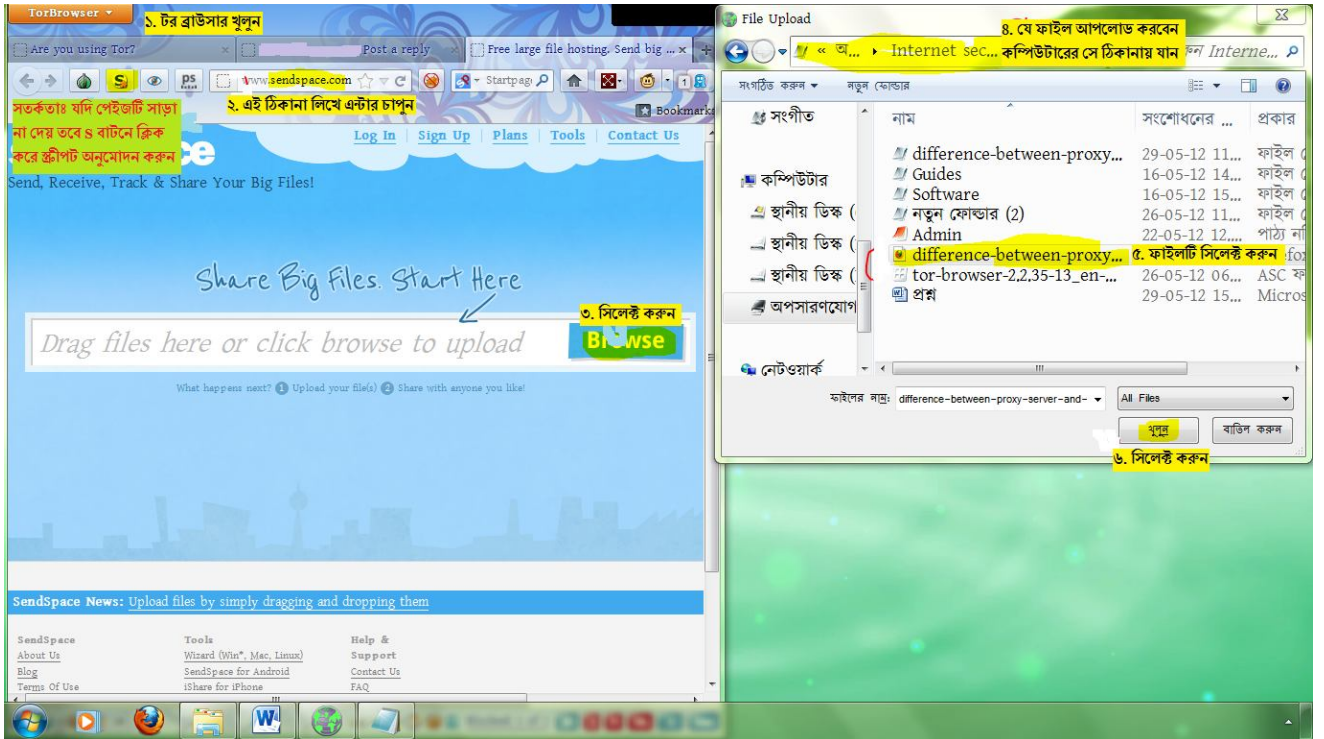
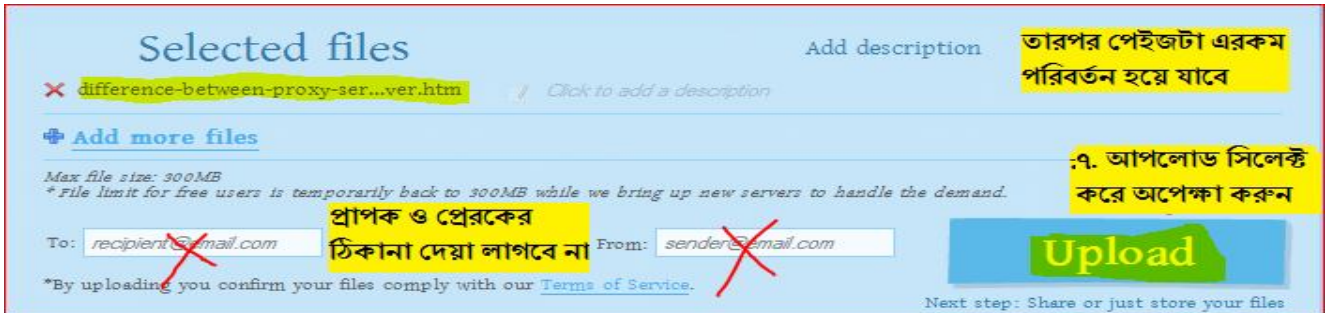
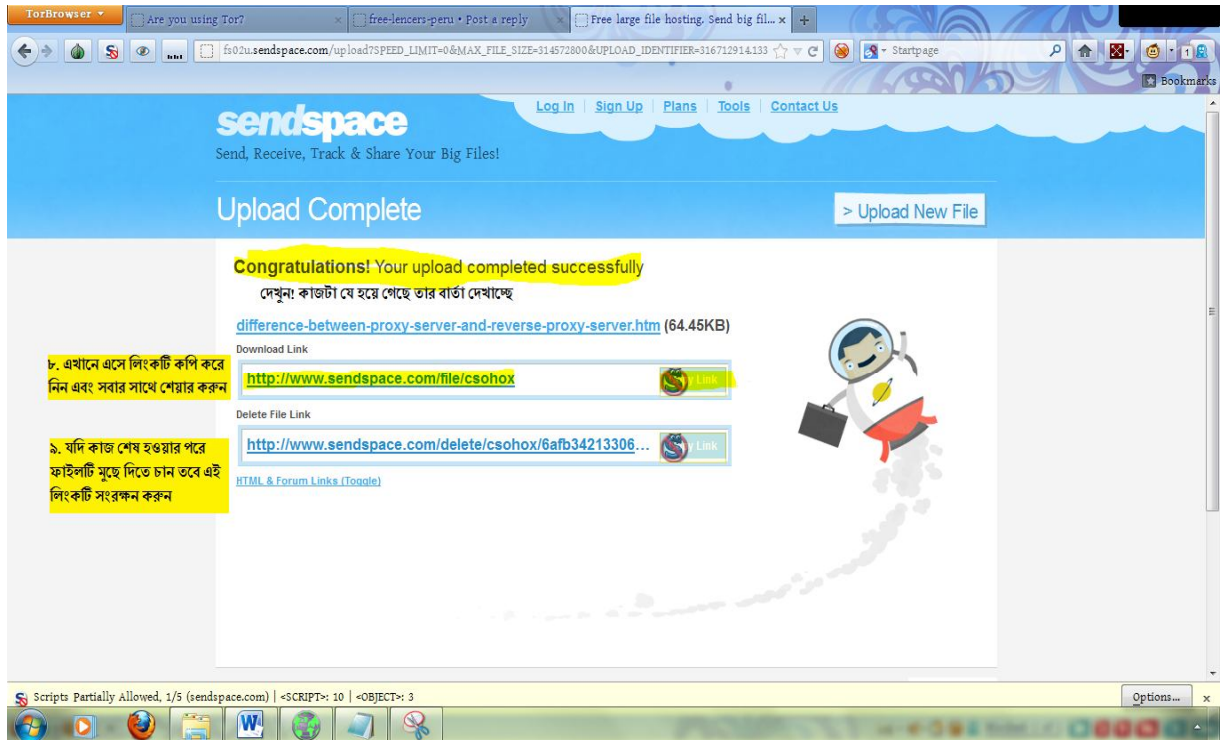
এরপর নীচের ছবি অনুযায়ী কাজ করুন।

Encrypt বাটনে ক্লিক করুন। মেসেজ রেডী হয়ে গেলে সেটাকে copy করুন।

এখন notepad এ paste করে উপরে ও নীচে asrar al mujahideen লিখা লাইন্গুলি মুছে দিন। এটা সতর্কতার জন্য। যাতে ইমেইলে পাঠানোর সময় কেউ স্ক্যান করে বুঝতে না পারে যে, এটা আসরার দিয়ে তৈরী একটি এনক্রিপ্টেড মেসেজ।

৪.৪. বার্তা ডিক্রিপ্ট করার পদ্ধতি

প্রথমে আপনার প্রাইভেট কী ও বার্তা প্রেরণকারীর পাবলিক কী সিলেক্ট করুন। তারপর Messaging বাটনে ক্লিক করুন।

Received Encrypted Message এ ক্লিক করুন ও নীচের ছবি অনুযায়ী কাজ করুন।

পাঠানো মেসেজ paste করে Decrypt বাটনে ক্লিক করুন।

পাঠানো মেসেজটি ডিক্রিপ্ট হয়ে যাবে।

৫. অন্যান্য গুরুত্বপূর্ণ কাজ

৫.১. ফাইল আপলোড করার পদ্ধতি

ফাইল আপলোড করার জন্য অনেক সাইট আছে। Google এ file share / upload লিখে সার্চ করলে এ রকম অনেক সাইট পাওয়া যাবে। নীচে www.sendspace.com এর মাধ্যমে ফাইল আপলোড করার পদ্ধতি দেখানো হলো।

প্রথমে টর ব্রাউসারে www.sendspace.com সাইটটি ওপেন করুন। এরপর Browse বাটনে ক্লিক করে আপনার প্রয়োজনীয় ফাইল সিলেক্ট করুন।

এরপর Upload বাটনে ক্লিক করুন।

ফাইল আপলোড হবার পর উপরের লিংকটি copy করে সবার সাথে শেয়ার করুন।

৫.২. শক্তিশালী পাসওয়ার্ড ব্যবহার

একটি ভালো পাসওয়ার্ড বানানোর নিয়ামাবলীঃ

i. ৮ ডিজিটের চেয়ে বেশি সংখ্যক অক্ষর ব্যবহার করুন।

ii. অর্থবোধক শব্দ বা, বাক্য ব্যবহার না করা।

iii. বড় হাতের ও ছোট হাতের অক্ষর ব্যবহার।

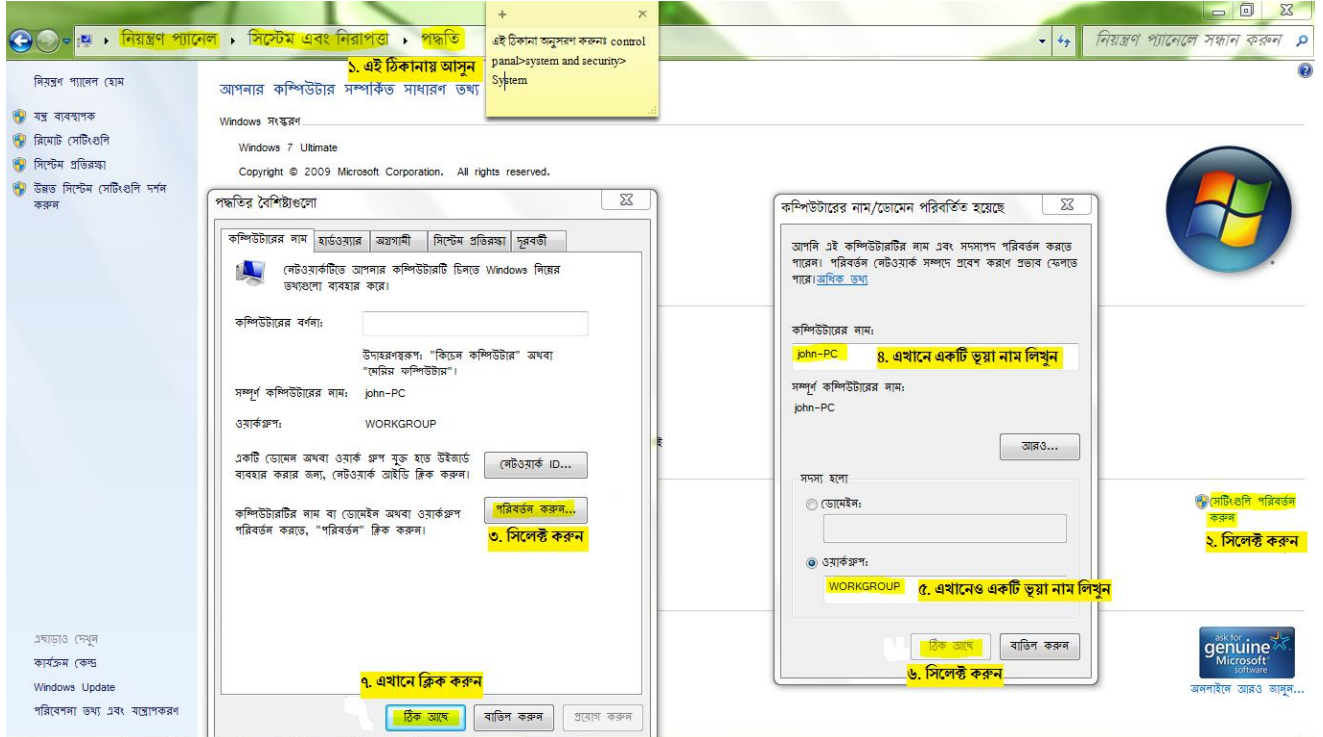
iv. অক্ষর, নম্বর ও প্রতীক এর সমন্বয়ে পাসওয়ার্ড তৈরী।

নীচে শক্তিশালী এবং দুর্বল পাসওয়ার্ডের ৩টি করে উদাহরণ দেয়া হলোঃ

শক্তিশালী পাসওয়ার্ড	দূর্বল পাসওয়ার্ড
GO&5#nd(+;26	Salmankhan
Jh(53)IbGj	123456
J^Ko*bRh%	Ilovetoeat

৫.৩. কম্পিউটারের নাম পরিবর্তন

আপনার Computer Name হিসেবে নিজের নাম কিংবা অন্য কোন পরিচিতি রাখবেন না।

কম্পিউটার নেম পরিবর্তনের জন্য My Computer এর উপর Right Click করুন। Properties ক্লিক করুন। Change Settings এ Change ক্লিক করুন। Computer Name পরিবর্তন করুন।

৫.৪. ওয়েব এড্রেস থেকে আই.পি. এড্রেস বের করা

ওয়েব এড্রেস ব্যবহার না করে সরাসরি আই পি এড্রেস ব্যবহার করা ভালো। যেমনঃ https://www.ansar1.info/ এর পরিবর্তে https://193.107.86.244/

ওয়েব এড্রেস থেকে আইপি এড্রেস ওয়েব সাইট http://tejji.com/ip/url-to-ip-address.aspx ব্যবহার করুন। এই সাইটে আপনার প্রয়োজনীয় এড্রেস লিখে Convert to IP ক্লিক করলে আইপি এড্রেস দেখাবে। একবার আপনার গন্তব্যের আইপি জানা হয়ে গেলে তা সংরক্ষণ করে রাখুন।

৫.৫. মডেম পরিবর্তন

পারলে কয়েক মাস পর পর মডেম পরিবর্তন করুন। মডেম যে অন্য নামে কিনতে হবে কিংবা রেজিঃ ছাড়া ব্যবহার করতে হবে সেটা বলাই বাহুল্য। সাধারণত মোবাইল কোম্পানীর মডেম ব্যবহার করা উচিত। যদিও সেখানে আপনি স্পীডকম পাবেন, তবে ব্রডবেন্ডের তুলনায় মনে হয় মোবাইল কোম্পানিগুলো কিছুটা নিরাপদ। কারণ তাদেরকে অনেক গ্রাহকের কল মনিটর করতে হয়। আপনার ইন্টারনেট ট্রাফিক মনিটর করা তাদের সেকেন্ড প্রায়োরিটি। কিন্তু আপনি যদি বাংলা লায়ন বা কিউবি নেন (ওয়াই ম্যাক্স) সে ক্ষেত্রে এই কোম্পানি গুলোর একমাত্র কাজ হচ্ছে আপনার ট্রাফিক মনিটর করা।

৫.৬. ডি.এন.এস. পরিষ্কার করা

Domain Name System সংক্ষেপে DNS নামে পরিচিত। এটি একটি ডাটাবেজ সিস্টেম। এটি একটি কম্পিউটারের ডমেইন নাম-কে আইপি এড্রেসে অনুবাদ করে। এর বিপরীত হল rDNS। যা একটি কম্পিউটারের আইপি এড্রেসকে ডমেইন নামে অনুবাদ করে। আপনি যখন কোন ওয়েবসাইটে যান, তখন আপনি ইউজার ফ্রেন্ডলি একটি নাম টাইপ করেন, যা হল সেটির ডমেইন নাম। যেমনঃ http://www.google.com। কিন্তু একটি নেটওয়ার্কে একটি কম্পিউটার অপরটির সাথে যুক্ত হবার জন্য আইপি এড্রেস ব্যবহার করে। যা হল একটি কম্পিউটারের প্রকৃত ঠিকানা। যেমনঃ 58.93.116.6। যার ফলে আপনি যখন ব্রাউজারের এড্রেস বারে কোন ডমেইন নাম লিখে এন্টার দেন, তখন তা ইন্টারনেটের DNS সিস্টেমের সাহায্য নেয়। তবে তা সরাসরি DNS সিস্টেমের সাথে যোগাযোগ করে না। এটি একটি DNS সার্ভারের সাথে যোগাযোগ করে। DNS সার্ভার হল এমন যে কোন কম্পিউটার, যা DNS সিস্টেমের সাথে যোগাযোগ করার জন্য রেজিস্টার করেছে। DNS সার্ভার কম্পিউটারটি DNS সিস্টেমের কাছে ক্লায়েন্টের পাঠানো ডমেইন নামটি দেয়। DNS সিস্টেমটি কাজের সুবিধার্থে DNS সার্ভার কম্পিউটার এবং ক্লায়েন্টের কম্পিউটার, উভয়টিতেই এভাবে পাঠানো ডমেইন নামের তালিকা এবং সংশ্লিষ্ট তথ্য সেভ করে দেয়। এই সেভ করা তথ্যকেই DNS cache বলে।

কিছুক্ষণ ইন্টারনেট ব্রাউজ করে Command Prompt এ ipconfig/displaydns লিখে এন্টার দিলে DNS cache-এ রাখা তথ্যগুলো আপনি দেখতে পাবেন। এই তথ্যগুলো ক্লিয়ার করার জন্য Command

Prompt এ ipconfig/flushdns লিখে এন্টার দিবেন। এতে আপনার কম্পিউটারটি DNS cache-এ রাখা তথ্যগুলো flush করে দিবে।